IMPLEMENTIERUNGSLEITFADEN

EMC VSPEX-ANWENDER-COMPUTING

VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO

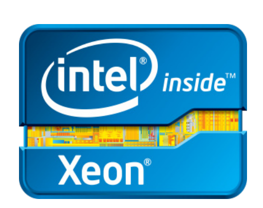
Unterstützt durch EMC Isilon, EMC VNX und EMC Datensicherheit

EMC VSPEX

Zusammenfassung

In diesem Implementierungsleitfaden werden die allgemeinen Schritte für die Bereitstellung einer EMC® VSPEX®-Lösung für Anwender-Computing für VMware Horizon View und VMware vSphere mit EMC XtremIO™ sowie EMC Isilon®, EMC VNX® und EMC Datensicherheit beschrieben.

März 2015



EMC²

Veröffentlicht im März 2015

EMC VSPEX-Anwender-Computing
VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO
Unterstützt durch EMC Isilon, EMC VNX und EMC Datensicherheit
Implementierungsleitfaden

Art.-Nr.: H13313.1



Inhalt





Abbildungen



Tabelle



Kapitel 1 Einführung

In diesem Kapitel werden die folgenden Themen behandelt:



Zweck dieses Leitfadens

Mit der EMC® VSPEX®-Architektur für Anwender-Computing (End-User Computing, EUC) erhält der Kunde ein modernes System, mit dem eine große Zahl virtueller Desktops auf einem konsistenten Performancelevel gehostet werden kann. Diese VSPEX-Lösung für Anwender-Computing mit VMware Horizon View 6.0 wird auf einer VMware vSphere-Virtualisierungsebene ausgeführt, die von der hochverfügbaren EMC XtremIO™-Produktreihe unterstützt wird, die den Speicher bereitstellt. In dieser Lösung werden die Komponenten der Desktopvirtualisierungsinfrastruktur auf einer VSPEX Private Cloud für VMware vSphere Proven Infrastructure ausgeführt, während die Desktops auf dedizierten Ressourcen gehostet werden.

Die von den VSPEX-Partnern definierten Rechner- und Netzwerkkomponenten sind redundant und ausreichend leistungsstark ausgelegt, um die Verarbeitungs- und Datenanforderungen einer großen virtuellen Maschinenumgebung zu erfüllen. EMC XtremIO-Arrays bieten Speicherplatz für virtuelle Desktops, EMC VNX®-Arrays bieten Speicher für Benutzerdaten, die EMC Avamar®-Backup- und Recovery-Optionen bieten Datensicherheit für VMware Horizon View-Daten und EMC RSA® SecurID® bietet optionale sichere Benutzerauthentifizierungsfunktionen.

Diese VSPEX Lösung für Anwender-Computing ist für virtuelle Desktops mit 2.500 vollständigen Clones oder 3.500 verknüpften Clones für einen X-Brick-Baustein und für virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder mit bis zu 1.750 verknüpften Clones für einen Starter-X-Brick-Baustein validiert. Die validierten Konfigurationen basieren auf einem Referenzdesktop-Workload und bilden die Basis für kostengünstige, benutzerdefinierte Lösungen für einzelne Kunden.

XtremIO unterstützt Scale-out-Cluster mit bis zu sechs X-Bricks. Jeder zusätzliche X-Brick-Baustein erhöht die Performance und virtuelle Desktopkapazität linear. XtremIO-X-Brick-Bausteine wurden für den Support einer höheren Anzahl von Desktops (mit vollständigen und mit verknüpften Clones) validiert und die Zahlen der VSPEX-Validierungen gelten nur für die hier vorgestellte Lösung.

Eine Infrastruktur für Anwender-Computing oder virtuelle Desktops ist ein komplexes Systemangebot. In diesem Implementierungsleitfaden wird beschrieben, wie Sie mithilfe von Best Practices die erforderlichen Ressourcen implementieren, um eine Anwender-Computing-Lösung unter Verwendung von VMware Horizon View für VMware vSphere mit Unterstützung durch XtremIO, EMC Isilon®, VNX und EMC Datensicherheit bereitzustellen.

Geschäftlicher Nutzen

Geschäftliche Anwendungen werden zunehmend in konsolidierte Rechner-, Netzwerk- und Speicherumgebungen verlagert. Diese VSPEX-Anwender-Computing-Lösung mit VMware reduziert die Komplexität bei der Konfiguration der einzelnen Komponenten eines herkömmlichen Bereitstellungsmodells. Durch diese Lösung wird das Integrationsmanagement vereinfacht. Gleichzeitig bleiben die Design- und Implementierungsoptionen von Anwendungen erhalten. Zudem werden die Administration vereinheitlicht und Kontrolle und Monitoring über die Prozesstrennung ermöglicht.



Die VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet unter anderem die folgenden geschäftlichen Vorteile:

- Bereitstellen einer End-to-End-Virtualisierungslösung zur Nutzung der Funktionen von einheitlichen Infrastrukturkomponenten
- Effiziente Virtualisierung für verschiedene Kundenanwendungsbeispiele
- Zuverlässige, flexible und skalierbare Referenzarchitekturen

Umfang

In diesem Implementierungsleitfaden werden die allgemeinen Schritte zur Bereitstellung der VSPEX-Lösung für Anwender-Computing für VMware Horizon View 6.0 beschrieben. Der Leitfaden liefert ein Bereitstellungsbeispiel eines virtuellen Desktopspeichers auf XtremIO und eines Benutzerdatenspeichers auf einem VNX-Speicherarray. Die für diese Lösung erforderlichen Infrastrukturserver wurden für die Ausführung auf einer VSPEX Private Cloud mit VMware vSphere Proven Infrastructure entworfen. Dieselben Prinzipien und Richtlinien gelten auch für die XtremIO-, Isilon- und VNX-Arrays, die im Rahmen des VSPEX-Programms von EMC validiert wurden.

Die EMC Datensicherheitslösungen für VMware Horizon View werden in einem separaten Dokument beschrieben: *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*.

Die optionale RSA® SecurID®-Lösung für sichere Benutzerauthentifizierung für VMware Horizon View wird in einem separaten Dokument beschrieben, *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: VMware Horizon View 5.2 und VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*.

Zielgruppe

Dieses Handbuch ist für internes EMC Personal und qualifizierte EMC VSPEX-Partner vorgesehen. In diesem Leitfaden wird davon ausgegangen, dass VSPEX-Partner, die beabsichtigen, diese VSPEX Proven Infrastructure für VMware Horizon View bereitzustellen, über die erforderliche Schulung und den entsprechenden Hintergrund verfügen, um eine Anwender-Computing-Lösung auf der Basis von Horizon View mit vSphere als Hypervisor, XtremIO-, Isilon- und VNX-Speichersysteme und die damit verbundene Infrastruktur installieren und konfigurieren zu können.

Leser sollten außerdem mit den Infrastruktur- und Datenbanksicherheitsrichtlinien der Kundeninstallation vertraut sein.

In diesem Leitfaden werden gegebenenfalls externe Referenzen bereitgestellt. Partner, die diese Lösung implementieren, sollten mit diesen Dokumenten vertraut sein. Weitere Informationen finden Sie unter Grundlegende Dokumente und Referenzdokumentation.

Terminologie

In Tabelle 1 führt die in diesem Handbuch verwendete Terminologie auf.

Tabelle 1. Terminologie

Begriff	Definition
Datendeduplizierung	Eine Funktion des XtremIO-Arrays, das die Auslastung des physischen Speichers reduziert, indem redundante Datenblöcke eliminiert werden.
Vollständige Clones	Desktops, die mittels vSphere-Vorlage bereitgestellt werden
Verknüpfte Clones	Desktops, die ein gemeinsames Basis-Image innerhalb eines Desktoppools verwenden und deshalb nur wenig Platz im Speicher belegen.
Referenzarchitektur	Die validierte Architektur, die diese VSPEX-Lösung für Anwender-Computing an vier bestimmten Skalierungspunkten unterstützt.
Referenz-Workload	Für VSPEX-Lösungen für Anwender-Computing wird der Referenz-Workload als ein einziger virtueller Desktop – der virtuelle Referenzdesktop – definiert, der die im Designleitfaden aufgeführte Workload-Konfiguration aufweist. Durch den Vergleich der tatsächlichen Auslastung des Kunden mit dem Referenz-Workload können Sie entscheiden, welche Referenzarchitektur Sie als Basis für Ihre VSPEX-Bereitstellung auswählen sollten. Weitere Informationen dazu finden Sie im Designleitfaden.



Kapitel 2 Bevor Sie beginnen

In diesem Kapitel werden die folgenden Themen behandelt:



Übersicht

In diesem Kapitel erhalten Sie einen Überblick über wichtige Informationen, die Sie kennen, Dokumente, mit denen Sie vertraut sein und Aufgaben, die Sie ausführen müssen, bevor Sie mit der Implementierung der VSPEX-EUC-Lösung für VMware Horizon View beginnen.

Im begleitenden Dokument für diese Lösung – *EMC VSPEX-Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO – Designleitfaden* – wird beschrieben, wie Sie Ihre Lösung entwerfen und dimensionieren, Ressourcen gemäß Best Practices zuweisen und alle Vorteile von VSPEX nutzen. Die Beispiele für Bereitstellungen in diesem Implementierungsleitfaden beruhen auf den Empfehlungen und Beispielen des Designleitfadens.

Aufgaben vor der Bereitstellung

Zu den Aufgaben vor der Bereitstellung zählen Verfahren, die nicht direkt mit der Installation und Konfiguration der Umgebung zusammenhängen, sondern deren Ergebnisse zum Zeitpunkt der Installation benötigt werden. Beispiele für Aufgaben vor der Bereitstellung sind das Sammeln von Hostnamen, IP-Adressen, VLAN-IDs, Lizenzschlüsseln, Installationsmedien und so weiter. Diese Aufgaben sollten vor dem Besuch beim Kunden erledigt werden, um den Zeitaufwand vor Ort so gering wie möglich zu halten.

Tabelle 2. Aufgaben vor der Bereitstellung

Aufgabe	Beschreibung	Referenz
Sammeln von Dokumenten	Sammeln Sie die in Grundlegende Dokumente und Referenzdokumentation aufgeführten Dokumente. Diese Dokumente werden im gesamten Implementierungsleitfaden dafür verwendet, Details zu Einrichtungsverfahren und Dimensionierung sowie Best Practices für die Bereitstellung der verschiedenen Komponenten der Lösung zur Verfügung zu stellen.	• Grundlegende Dokumente • Referenzdokumentation
Sammeln von Tools	Sammeln Sie die erforderlichen und optionalen Tools für die Bereitstellung. Mit Tabelle 4 auf Seite 17 können Sie prüfen, ob die gesamte Hardware und Software und die entsprechenden Lizenzen vor dem Bereitstellungsprozess verfügbar sind.	Tabelle 4, Checkliste für die Bereitstellungsvoraussetzungen



Aufgabe	Beschreibung	Referenz
Sammeln von Daten	Sammeln Sie die kundenspezifischen Konfigurationsdaten für Netzwerk, Arrays, Konten usw. Geben Sie diese Informationen in das Arbeitsblatt für die Kundenkonfiguration ein, das Sie während des Bereitstellungsprozesses als Referenz verwenden können. Füllen Sie zusätzlich die relevante XtremIO-Checkliste für Aufgaben vor der Installation und das VNX-Arbeitsblatt aus, um umfassende arrayspezifische Informationen zur Hand zu haben. Diese Dokumente stehen auf der EMC Online Support-Website zur Verfügung.	• *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation* • *EMC VNX Installation Assistant for File/Unified-Arbeitsblatt* • Arbeitsblatt für die Kundenkonfiguration

Bereitstellungsworkflow

Ziehen Sie für das Design und die Implementierung Ihrer Anwender-Computing-Lösung den Prozessablauf in Tabelle 3 zurate.

Tabelle 3. Bereitstellungsworkflow

Schritt	Aktion
1	Verwenden Sie das Arbeitsblatt für die Kundenkonfiguration im Designleitfaden, um Kundenanforderungen zu erfassen.
2	Verwenden Sie das EMC VSPEX-Dimensionierungstool, um die empfohlene VSPEX-Referenzarchitektur für Ihre Anwender-Computing-Lösung auf der Basis der in Schritt 1 erfassten Benutzeranforderungen zu ermitteln. Weitere Informationen zum Dimensionierungstool finden Sie unter VSPEX-Dimensionierungstool. **Hinweis**: Sollte das Dimensionierungstool nicht zur Verfügung stehen, können Sie die Anwendung anhand der Richtlinien im Designleitfaden manuell dimensionieren.
3	Legen Sie das endgültige Design der VSPEX-Lösung mithilfe des Designleitfadens fest. **Hinweis**: Sorgen Sie dafür, dass alle Ressourcenanforderungen und nicht nur die Anforderungen für das Anwender-Computing berücksichtigt werden.
4	Wählen Sie die geeignete VSPEX-Referenzarchitektur und Proven Infrastructure aus und bestellen Sie sie. Im Dokument *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen – Handbuch zur Proven Infrastructure-Lösung* finden Sie Anweisungen zur Auswahl einer Proven Infrastructure für die VSPEX Private Cloud.
5	Befolgen Sie diesen Implementierungsleitfaden zum Bereitstellen und Testen Ihrer VSPEX-Lösung. **Hinweis**: Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie die bereits abgeschlossenen Implementierungsschritte überspringen.

Grundlegende Dokumente

EMC empfiehlt, die folgenden Dokumente zu lesen, die Sie im Bereich „VSPEX“ im EMC Community Network, unter http://germany.emc.com oder im VSPEX Proven Infrastructure-Partnerportal finden.

Übersicht über die Lösungen von VSPEX

Weitere Informationen zur VSPEX-Lösungsübersicht finden Sie in der *Übersicht zur EMC VSPEX-Lösung für Anwender-Computing mit VMware vSphere und VMware View.*

VSPEX-Designleitfaden

Weitere Informationen finden Sie im *EMC VSPEX für Anwender-Computing: VMware Horizon View 6.0 und VMware vSphere mit EMC XtremIO – Designleitfaden.*



VSPEX Proven Infrastructure-Leitfaden

Im Dokument *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen – Handbuch zur Proven Infrastructure-Lösung* finden Sie weitere Informationen bezüglich einer VSPEX Proven Infrastructure.

Leitfaden: EMC Backup und Recovery für VSPEX

Weitere Informationen zu EMC Datensicherheit für VSPEX finden Sie im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View.*

Voraussetzungen für die Bereitstellung

In Tabelle 4 gibt die Hardware-, Software- und Lizenzanforderungen für die Konfiguration der Lösung an. Weitere Informationen zu diesen Anforderungen finden Sie auf der EMC Online Support-Website.

Tabelle 4. Checkliste für die Bereitstellungsvoraussetzungen

Anforderung	Beschreibung
Hardware	• Physische Server mit ausreichend Kapazität zum Hosten der virtuellen Desktops gemäß den Empfehlungen im Designleitfaden • VMware vSphere-Server zum Hosten der virtuellen Infrastrukturserver • Für das Anwender-Computing erforderliche Netzwerkswitch-Portkapazität und -funktionen • EMC XtremIO-Array mit der erforderlichen Konfiguration • EMC Isilon mit der erforderlichen Konfiguration • EMC VNX-Multiprotokoll-Speicherarray mit dem erforderlichen Laufwerkslayout **Hinweis**: Diese Anforderungen werden möglicherweise durch die vorhandene Infrastruktur erfüllt.
Software	• Installationsmedien für VMware vSphere 5.5 • Installationsmedien für VMware vCenter Server 5.5 • VMware vShield Manager Open Virtualization Appliance (OVA)-Datei • VMware vRealize Operations Manager OVA-Datei • VMware vRealize Operations Manager for Horizon View Adapter • Installationsmedien für VMware Horizon View 6.0 • Management-Serversoftware für die VMware vShield Endpoint-Virenschutzlösung von Partnern • VMware vShield Endpoint-Partnersoftware für die Sicherheit von virtuellen Maschinen • OVA-Datei für EMC XtremIO Management Server • EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client • EMC VSI für VMware vSphere Storage Viewer • EMC PowerPath® Viewer • EMC PowerPath/VE • Installationsmedien für Microsoft Windows Server 2012 R2 (empfohlenes Betriebssystem für VMware vCenter und VMware Horizon View Connection Server) • Installationsmedien für Microsoft Windows 7.0 oder Windows 8.1 • Installationsmedien für Microsoft SQL Server 2012 oder höher **Hinweis**: Diese Anforderung wird möglicherweise durch die vorhandene Infrastruktur erfüllt.

Anforderung	Beschreibung
Lizenzen	• Lizenzschlüssel für VMware vSphere 5.5 (Infrastruktur-Serverhosts) • Lizenzschlüssel für VMware vCenter Server 5.5 • Lizenzschlüssel für VMware vSphere Desktop (virtuelle Desktophosts) • Lizenzschlüssel für VMware Horizon View 6.0 • Lizenzschlüssel für VMware vShield Endpoint (VMware) • Lizenzschlüssel für VMware vShield Endpoint (vShield-Partner) • Lizenzschlüssel für VMware vRealize Operations Manager • Lizenzschlüssel für Microsoft Windows Server 2012 R2 Standard Edition (oder höher) • Lizenzschlüssel für Microsoft Windows 7.0 oder Windows 8.1 • Lizenzschlüssel für Microsoft SQL Server 2012 **Hinweis**: Diese Lizenzanforderungen werden eventuell von vorhandenen Microsoft Key Management Servern (KMS) oder anderen Lizenzen abgedeckt. • Lizenzdateien für EMC PowerPath/VE



Kapitel 3 Lösungsüberblick

In diesem Kapitel werden die folgenden Themen behandelt:



Übersicht

In diesem Kapitel finden Sie einen Überblick über die VSPEX-Lösung für Anwender-Computing für VMware Horizon View mit VMware vSphere und die wichtigsten in der Lösung verwendeten Technologien. Die Lösung wurde von EMC entwickelt und erprobt und bietet die für die Unterstützung von Referenzarchitekturen mit virtuellen Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones für einen X-Brick-Baustein und mit virtuellen Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones für einen Starter-X-Brick-Baustein erforderlichen Ressourcen für Desktopvirtualisierung, Server, Netzwerk, Speicher und Backup.

XtremIO-X-Brick-Bausteine wurden für den Support einer höheren Anzahl von Desktops validiert (mit vollständigen und mit verknüpften Clones). Die Zahlen der VSPEX-Validierungen gelten nur für die hier vorgestellte Lösung.

Obwohl die Desktopvirtualisierungs-Infrastrukturkomponenten der Lösung in Abbildung 3 auf Seite 23 dafür entwickelt wurden, auf einer VSPEX Private Cloud-Lösung angelegt zu werden, umfassen die Referenzarchitekturen keine Konfigurationsdetails für die zugrunde liegende Proven Infrastructure. Im Dokument *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen – Handbuch zur Proven Infrastructure-Lösung* finden Sie Informationen zum Konfigurieren der erforderlichen Infrastrukturkomponenten.

VSPEX Proven Infrastructures

EMC hat gemeinsam mit den Anbietern von IT-Infrastrukturen eine vollständige Virtualisierungslösung entwickelt, die die Bereitstellung der Private Cloud und der virtuellen VMware Horizon View-Desktops beschleunigt. Mit VSPEX sind Kunden in der Lage, die Umgestaltung ihrer IT durch schnellere Bereitstellung, verbesserte Anwenderfreundlichkeit, größere Auswahl, höhere Effizienz und weniger Risiko zu beschleunigen. Dadurch wird die Erstellung der IT-Infrastruktur vereinfacht.

Die VSPEX-Validierung durch EMC ermöglicht eine zuverlässige Performance und ermöglicht Kunden die Auswahl von Technologien, die ihre vorhandene oder neu erworbene IT-Infrastruktur nutzen und so den Planungs-, Dimensionierungs- und Konfigurationsaufwand vermeiden. VSPEX stellt eine virtuelle Infrastruktur für Kunden bereit, die die charakteristische Einfachheit von echten konvergenten Infrastrukturen und gleichzeitig mehr Auswahlmöglichkeiten bei den einzelnen Stapelkomponenten erreichen möchten.

VSPEX Proven Infrastructures, wie in Abbildung 1 gezeigt, sind modulare und virtualisierte Infrastrukturen, die von EMC validiert und von EMC VSPEX-Partnern geliefert werden. Sie umfassen die Virtualisierungs-, Server-, Netzwerk-, Speicher- und Backupebene. Partner können die Virtualisierungs-, Server- und Netzwerktechnologien auswählen, die am besten zur Umgebung eines Kunden passen. Gleichzeitig stellen die Speichersysteme der hochverfügbaren XtremIO-, Isilon- und VNX-Produktreihe und EMC Datensicherheitstechnologien die Speicher- und Datensicherheitsebene zur Verfügung.



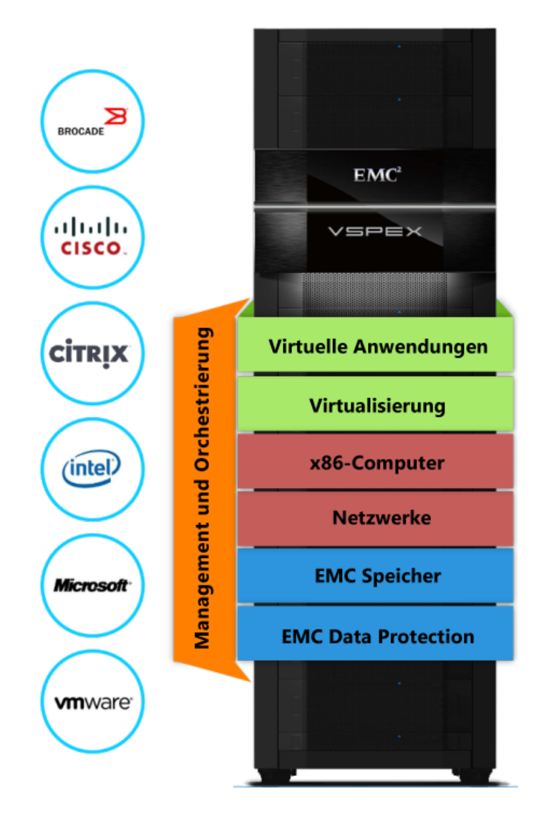


Abbildung 1. VSPEX Proven Infrastructures

Lösungsarchitektur

High-Level-Architektur

Die EMC VSPEX-Lösung für Anwender-Computing für VMware Horizon View bietet eine vollständige Systemarchitektur mit zwei XtremIO-X-Brick-Bausteinkonfigurationen. Ein XBrick kann virtuelle Desktops mit bis zu 2.500 vollständigen Clones oder 3.500 verknüpften Clones hosten, ein Starter-X-Brick kann virtuelle Desktops mit bis zu 1.250 vollständigen Clones oder 1.750 verknüpften Clones hosten. Die Lösung unterstützt Blockspeicher auf XtremIO für virtuelle Desktops und optionale Dateispeicher auf Isilon oder VNX für Benutzerdaten.

Abbildung 2 zeigt die allgemeine Architektur der validierten Lösung.

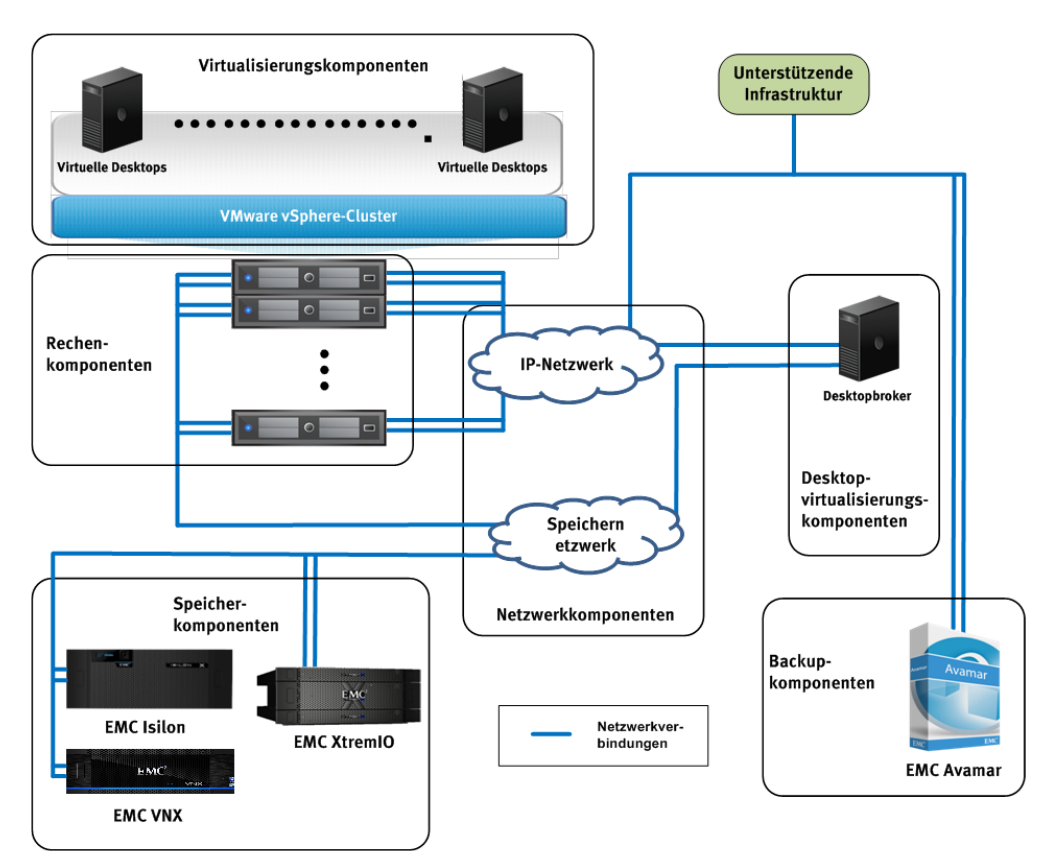


Abbildung 2. Architektur der validierten Lösung

Diese Lösung verwendet EMC XtremIO, Isilon oder VNX und vSphere für die Bereitstellung der Speicher- und Virtualisierungsplattformen für eine Horizon View-Umgebung mit virtuellen, von VMware View Composer bereitgestellten Microsoft Windows 7.0- oder Windows 8.1-Desktops.

Für diese Lösung haben wir[1] das XtremIO-Array in mehreren Konfigurationen bereitgestellt, um bis zu 3.500 virtuelle Desktops zu unterstützen. Wir haben die folgenden XtremIO-Arrays getestet:

- Ein Starter X-Brick-Baustein, der zum Hosten von virtuellen Desktops mit 1.250 vollständigen Clones oder 1.750 verknüpften Clones verwendet wurde
- Ein vollständiger X-Brick-Baustein, der zum Hosten von virtuellen Desktops mit 2.500 vollständigen Clones oder 3.500 verknüpften Clones verwendet wurde

Wir haben auch ein Isilon-Cluster und ein VNX-Array für das Hosten von Benutzerdaten bereitgestellt.

Die Infrastrukturservices für die Lösung, die in Abbildung 3 dargestellt sind, können durch eine vorhandene Infrastruktur am Kundenstandort, durch die VSPEX Private Cloud oder durch die Bereitstellung der Services als dedizierte Ressourcen im Rahmen der Lösung bereitgestellt werden. Für das virtuelle Desktopcluster sind dedizierte Anwender-Computing-Ressourcen erforderlich. Eine Ausführung des Clusters in einer VSPEX Private Cloud ist nicht vorgesehen.

[1] In diesem Leitfaden bezieht sich „wir“ auf das EMC VSPEX-Technikerteam, das die Lösung validiert hat.



Die Planung und das Design der Speicherinfrastruktur für die Horizon View-Umgebung ist ein wichtiger Schritt, da der gemeinsame Speicher in der Lage sein muss, große Belastungsspitzen bei I/O-Vorgängen abzufangen, die im Laufe eines Tages auftreten. Diese Belastungsspitzen können zu Phasen mit einer unregelmäßigen und unzuverlässigen Performance der virtuellen Desktops führen. Benutzer gewöhnen sich möglicherweise an eine langsame Performance, aber eine unzuverlässige Performance führt zu Frustration und verringert die Effizienz.

Für eine zuverlässige Performance in einer Anwender-Computing-Lösung muss das Speichersystem die Spitzen-I/O-Last der Clients bei minimaler Antwortzeit verarbeiten können. Diese Lösung verwendet das XtremIO-Array, um die Antwortzeiten unter einer Millisekunde zu ermöglichen, die Kunden benötigen, während die Echtzeit-Inline-Deduplizierungsfunktionen der Plattform den benötigten physischen Speicher verringern.

EMC Data Protection-Lösungen ermöglichen den Schutz von Benutzerdaten und die Wiederherstellbarkeit durch Anwender. Dafür werden in dieser Horizon View-Lösung Avamar Backup und Recovery und der damit verbundene Desktopclient verwendet.

Logische Architektur

Die Lösung unterstützt Blockspeicher für die virtuellen Desktops. Abbildung 3 zeigt die logische Architektur der Lösung.

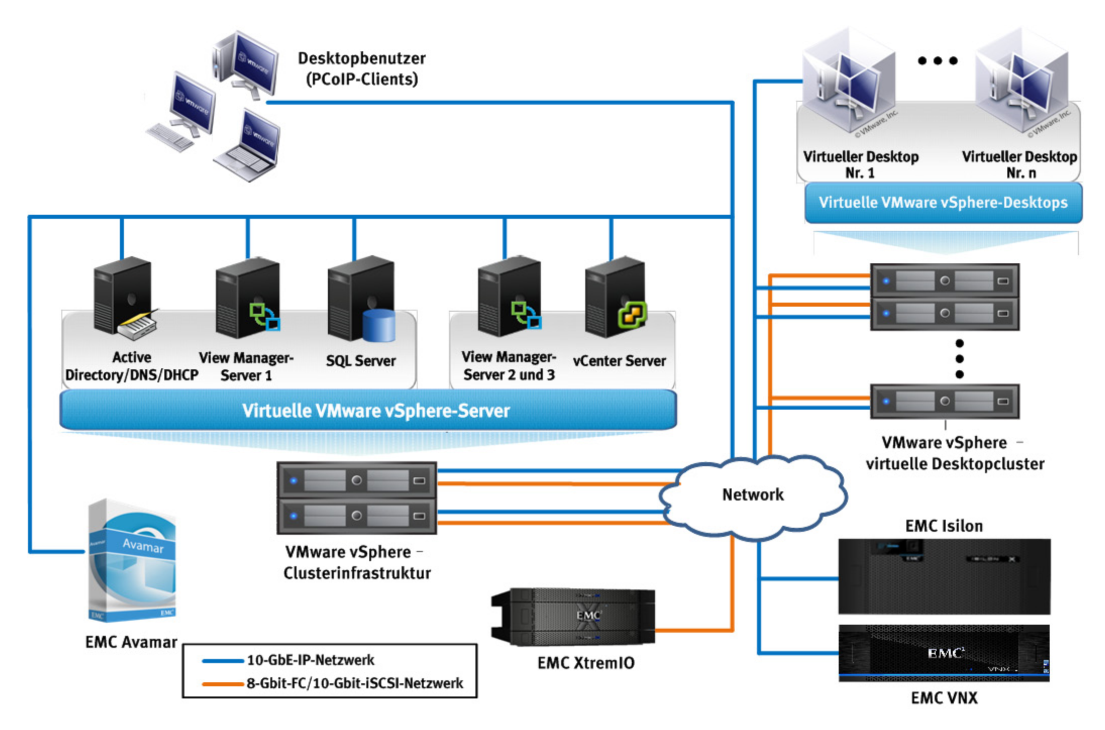


Abbildung 3. Logische Architektur

Diese Lösung verwendet zwei Netzwerke: ein Speichernetzwerk zur Bereitstellung von virtuellen Desktops und virtuellen Serverbetriebssystemdaten sowie ein 10-Gbit-Ethernetnetzwerk (GbE) für den übrigen Datenverkehr. Für das Speichernetzwerk wird 8-Gbit-Fibre-Channel (FC) oder 10 GbE mit iSCSI-Protokoll verwendet.

Hinweis: Die Lösung unterstützt darüber hinaus 1 GbE, falls die Bandbreitenanforderungen erfüllt werden.



Übersicht über die wichtigen Komponenten

In Tabelle 5 fasst die in dieser Lösung verwendeten Kerntechnologien zusammen. Der Implementierungsleitfaden bietet einen Überblick über die einzelnen Komponenten.

Tabelle 5. Lösungskomponenten

VSPEX-Ebene	Komponenten
Anwendungsebene	• Desktop-Virtualisierungs-Broker von VMware Horizon View 6.0 mit den folgenden Komponenten: ▪ VMware View Manager ▪ VMware View Composer ▪ VMware Horizon View Persona Management ▪ VMware Horizon View Storage Accelerator ▪ VMware vRealize Operations Manager für Horizon View • VMware Workspace
Virtualisierungsebene	• VMware vSphere-Hypervisor mit den folgenden Komponenten: ▪ VMware vSphere ▪ VMware vCenter Server ▪ VMware vSphere High Availability • VMware vShield Endpoint
Rechnerebene	Jede Serverhardware, die die Mindestanforderungen erfüllt, die durch VSPEX definiert sind
Netzwerkebene	Jede Netzwerkhardware, die die Mindestanforderungen erfüllt, die durch VSPEX definiert sind **Hinweis**: VSPEX definiert die Mindestanzahl der für die Lösung erforderlichen Netzwerkports und stellt allgemeine Anweisungen für die Netzwerkarchitektur bereit.
Speicherebene	• EMC XtremIO mit den folgenden Komponenten: ▪ EMC XtremIO Management Server ▪ EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client ▪ VMware vSphere Storage APIs for Array Integration ▪ EMC XtremIO Snapshots • EMC VNX-Serie mit den folgenden Komponenten: ▪ EMC Unisphere® Management Suite ▪ EMC VSI for VMware vSphere ▪ VMware vSphere Storage APIs for Array Integration ▪ VMware vSphere Storage APIs for Storage Awareness ▪ EMC VNX Snapshots ▪ EMC SnapSure™ ▪ EMC VNX Virtual Provisioning ▪ EMC Fully Automated Storage Tiering (FAST™) Suite – FAST-Cache und FAST für virtuelle Pools (FAST VP)
Backup- und Recovery-Ebene	EMC Avamar
Sicherheitsschicht	EMC RSA SecurID



Kapitel 4 Lösungsimplementierung

In diesem Kapitel werden die folgenden Themen behandelt:



Übersicht

In diesem Kapitel wird beschrieben, wie die Referenzarchitektur der EUC-Lösung implementiert wird. Wenn Sie bereits über eine VSPEX Proven Infrastructure-Umgebung verfügen, können Sie Abschnitte mit den schon abgeschlossenen Schritten für die Implementierung überspringen. Andernfalls finden Sie Informationen zum Konfigurieren der erforderlichen Infrastrukturkomponenten im *EMC VSPEX Private Cloud: VMware vSphere 5.5 für bis zu 1.000 virtuelle Maschinen – Proven Infrastructure-Leitfaden*.

Hinweis: Diese Lösung erfordert bestimmte Infrastrukturservices, wie in Abbildung 3 auf Seite 23 gezeigt. Diese Services können auch von einer vorhandenen Infrastruktur am Kundenstandort, durch eine VSPEX Private Cloud oder durch ihre Bereitstellung als dedizierte Ressourcen für diese Lösung bereitgestellt werden.

In Tabelle 6 listet die Hauptphasen des Implementierungsprozesses der Lösung auf und stellt Links zu den relevanten Abschnitten in diesem Kapitel bereit.

Tabelle 6. Überblick über den Implementierungsprozess

Phase	Beschreibung	Referenz
1	Konfiguration der Switche und Netzwerke und Herstellen einer Verbindung zum Kundennetzwerk	Implementieren der Netzwerkinfrastruktur
2	Installation und Konfiguration der XtremIO- und VNX-Arrays	Vorbereiten und Konfigurieren der Speicherarrays
3	Konfigurieren der Datastores der virtuellen Maschinen	
4	Installieren und Konfigurieren der Server	Installieren und Konfigurieren der vSphere-Hosts
5	Einrichten von SQL Server (verwendet von vCenter und Horizon View)	Installieren und Konfigurieren der SQL Server-Datenbank
6	Installieren und Konfigurieren von vCenter und des Netzwerks der virtuellen Maschine	Bereitstellen von VMware vCenter Server
7	Einrichten des View-Verbindungsservers	Einrichten von View Connection Server
8	Provisioning von virtuellen Desktops	Provisioning von virtuellen Desktops
9	Richten Sie EMC Avamar ein.	Einrichten von EMC Avamar
10	Einrichten von vShield Endpoint	Einrichten von VMware vShield Endpoint
11	Einrichten von VMware Workspace	Einrichten von VMware
12	Einrichten von VMware vRealize Operations Manager for Horizon View	Einrichten von VMware vRealize Operations Manager for

Implementieren der Netzwerkinfrastruktur

In diesem Abschnitt werden die Anforderungen für die Vorbereitung der Netzwerkinfrastruktur beschrieben, die zur Unterstützung dieser Lösung erforderlich ist. In Tabelle 7 enthält eine Zusammenfassung der abzuschließenden Aufgaben sowie Referenzen zu weiteren Informationen.

Tabelle 7. Aufgaben für die Switch- und Netzwerkkonfiguration

Aufgabe	Beschreibung	Referenz
Konfigurieren des Infrastrukturnetzwerks	Konfigurieren Sie das Speicherarray und das vSphere-Hostinfrastrukturnetzwerk.	Konfigurieren des Infrastrukturnet-zwerks
Konfigurieren der VLANs	Konfigurieren Sie private und öffentliche VLANs nach Bedarf.	Konfigurationsleitfaden Ihres Switchanbieters
Konfigurieren Sie das Speichernetzwerk.	Konfigurieren Sie die FC-Switchports, das Zoning für vSphere-Hosts und das Speicherarray.	• Konfigurieren Sie das Speichernetzwerk. • Konfigurationsleitfaden Ihres Switchanbieters
Vervollständigen der Netzwerkverkabelung	Verbinden Sie die Switchverbindungsports, die VNX-Ports, die Isilon-Ports und die vSphere-Serverports.	Vervollständigen der Netzwerkver-kabelung

Konfigurieren des Infrastrukturnet-zwerks

Das Infrastrukturnetzwerk erfordert redundante Netzwerkverbindungen für jeden vSphere-Host, das Speicherarray, die Switchverbindungsports und die Switch-Uplink-Ports. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Netzwerkbandbreite bereit.

Diese Konfiguration ist erforderlich, unabhängig davon, ob die Netzwerkinfrastruktur für die Lösung bereits vorhanden ist oder mit anderen Komponenten der Lösung bereitgestellt wird.

Abbildung 4 zeigt ein Beispiel einer redundanten Ethernetinfrastruktur für die in dieser Lösung verwendete VNX. Diese Lösung verwendet redundante Switche und Verbindungen, um sicherzustellen, dass kein Single-Point-of-Failure in der Netzwerkverbindung vorhanden ist. Dasselbe Prinzip gilt für eine Isilon-Konfiguration.

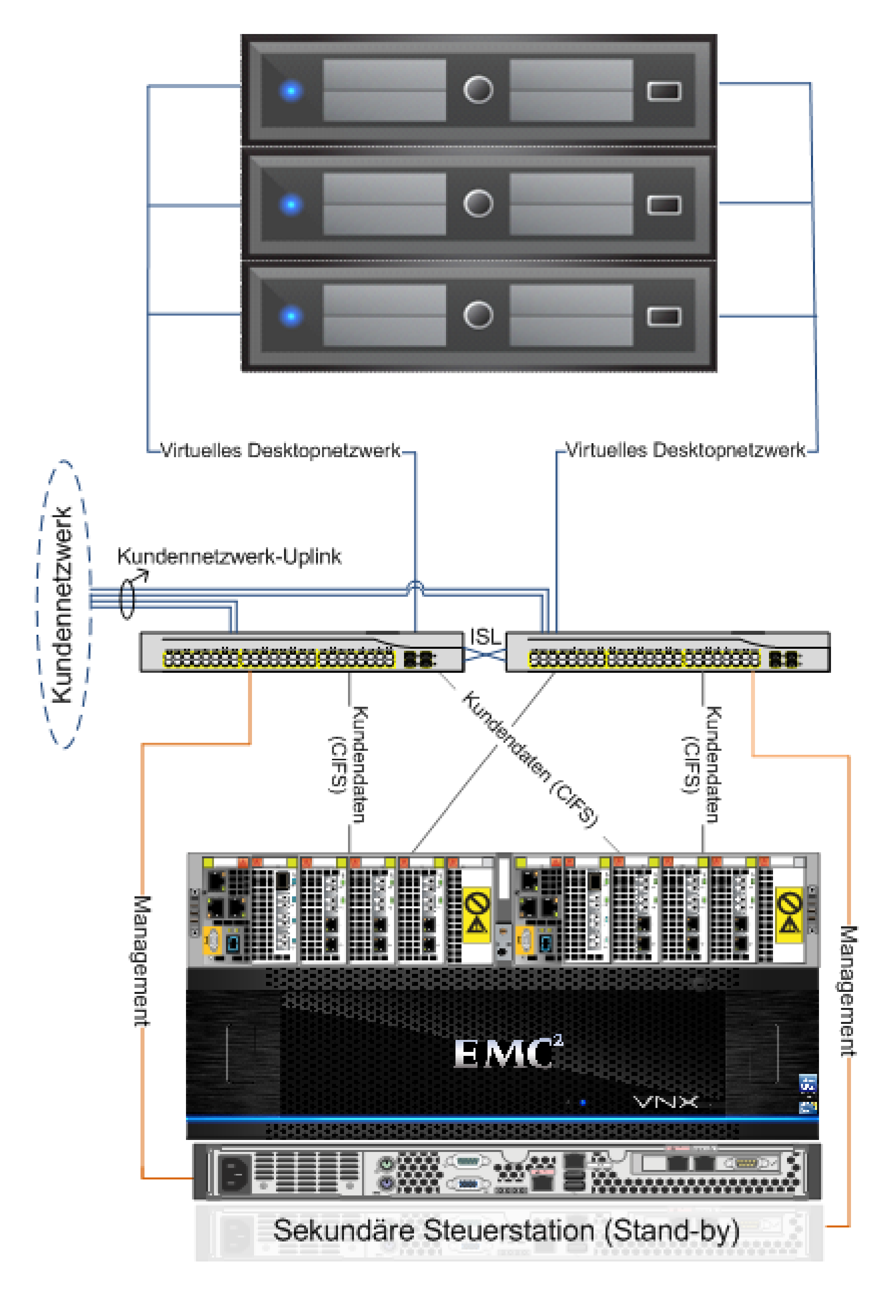


Abbildung 4. Beispiel-Ethernetnetzwerkarchitektur

Konfigurieren der VLANs

Achten Sie darauf, dass die Infrastruktur über eine geeignete Anzahl von Switchports für das Speicherarray und vSphere-Hosts verfügt. EMC empfiehlt, die folgenden vSphere-Hosts mit mindestens zwei virtuellen LANs zu konfigurieren:

- **Clientzugriffsnetzwerk:** Netzwerkverbindungen für virtuelle Maschinen und CIFS-Datenverkehr (kundenorientierte Netzwerke, die bei Bedarf getrennt werden können)
- **Managementnetzwerk:** vSphere-Management und VMware vMotion (privates Netzwerk)



Konfigurieren Sie das Speichernetzwerk.

Diese Lösung benötigt ein dediziertes Speichernetzwerk. Wenn iSCSI verwendet wird, um das XtremIO-Array mit vSphere-Hosts zu verbinden, ist ein dediziertes VLAN für das Speichernetzwerk erforderlich. Wenn FC oder eine Kombination aus FC beim XtremIO-Array und FCoE bei den vSphere-Hosts verwendet wird, sind keine weiteren VLANs für das Speichernetzwerk erforderlich.

Für die Lösungstests haben wir ein FC-Netzwerk verwendet. Für das Infrastruktur-Fibre-Channel-Netzwerk sind redundante Fibre-Channel-Switche sowie Links für jeden vSphere-Host und das Speicherarray erforderlich. Diese Konfiguration stellt sowohl Redundanz als auch zusätzliche Speichernetzwerkbandbreite bereit. Wir haben jeden vSphere-Host mit beiden Fibre-Channel-Switchen und jeden Switch mit jedem Speicherprozessor auf dem Speicherarray verbunden. Wir haben dann jede der Fibre-Channel-Verbindungen zwischen dem vSphere-Host und dem Speicherarray in eine separate Fibre-Channel-Zone platziert.

Abbildung 5 zeigt die für das Testen dieser Lösung verwendete Netzwerkarchitektur.

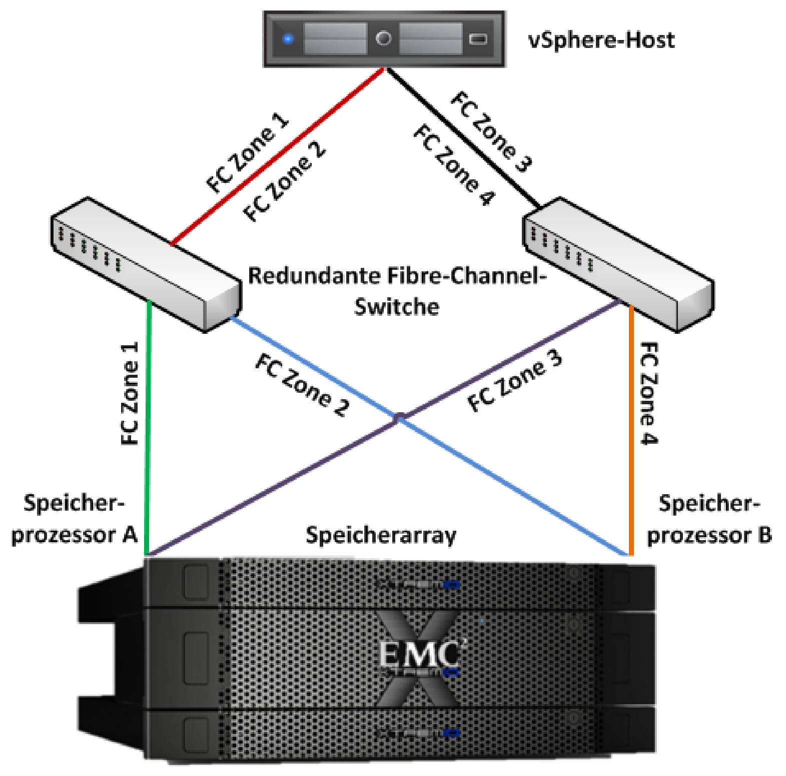


Abbildung 5. Beispiel für eine Fibre-Channel-Netzwerkarchitektur

Vervollständigen der Netzwerkverkabelung

Sorgen Sie dafür, dass alle Lösungsserver, Speicherarrays, Switchverbindungen und Switch-Uplinks über redundante Verbindungen verfügen und in separate Switching-Infrastrukturen eingesteckt sind. Sorgen Sie auch dafür, dass eine vollständige Verbindung zum vorhandenen Kundennetzwerk besteht.

Hinweis: Nach der Überprüfung, ob die neue Hardware mit dem vorhandenen Kundennetzwerk verbunden ist, vergewissern Sie sich, dass unvorhergesehene Interaktionen keine Serviceprobleme im Kundennetzwerk hervorrufen.

Vorbereiten und Konfigurieren der Speicherarrays

In diesem Abschnitt wird beschrieben, wie Sie die XtremIO-, Isilon- und VNX-Speicherarrays konfigurieren, die in dieser Lösung verwendet werden. Das XtremIO-Array stellt VMware Virtual Machine File System (VMFS)-Datenspeicher für Hosts zur Verfügung, während das optionale VNX- oder Isilon-Array CIFS-Speicher für Benutzerdaten bietet.

Alle in diesem Kapitel beschriebenen Beispiele für die Speicherkonfiguration gelten für die Konfigurationen mit zwei X-Brick-Bausteinen, die in dieser Lösung validiert sind. Wenden Sie sich für weitere Informationen zu größeren Konfigurationen an Ihren EMC Vertriebsmitarbeiter.

In Tabelle 8 zeigt die Aufgaben für die Speicherkonfiguration.

Tabelle 8. Aufgaben für die Speicherkonfiguration

Aufgabe	Beschreibung	Referenz
Bereiten Sie die XtremIO vor.	Installieren Sie die XtremIO-Hardware gemäß der Produktdokumentation.	*EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*
Vorbereiten des Isilon-Clusters	Installieren Sie die Isilon-Hardware gemäß der Produktdokumentation.	*Leitfaden für Isilon-Standortplanung und -vorbereitung*
Bereiten Sie die VNX vor.	Installieren Sie die VNX-Hardware gemäß der Produktdokumentation.	*VSPEX Private Cloud Proven Infrastructure-Leitfaden*
Einrichten der anfänglichen XtremIO-Konfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der XtremIO.	*EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
Einrichten der anfänglichen Isilon-Konfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der Isilon.	*Leitfaden für Isilon-Standortplanung und -vorbereitung*
Einrichten der anfänglichen VNX-Konfiguration	Konfigurieren Sie die IP-Adressinformationen und andere wichtige Parameter auf der VNX.	*VSPEX Private Cloud Proven Infrastructure-Leitfaden*
Speicher-Provisioning für VMFS-Datastores	Erstellen Sie XtremIO-Volumes, die den vSphere-Servern als VMFS-Datastores angezeigt werden, die die virtuellen Desktops hosten.	Speicher-Provisioning für VMFS-Datastores
FAST Cache konfigurieren	Konfigurieren Sie FAST Cache. Konfigurieren Sie optional FAST VP.	• VNX FAST Cache konfigurieren • Konfigurieren von FAST VP für Benutzerdaten auf VNX (optional)

Aufgabe	Beschreibung	Referenz
Provisioning von optionalem Speicher für Benutzerdaten	Erstellen Sie CIFS-Dateisysteme, die zum Speichern von Roaming-Benutzerprofilen und Stammverzeichnissen verwendet werden.	Provisioning von optionalem Speicher für Benutzerdaten
Provisioning von optionalem Speicher für virtuelle Infrastrukturmaschinen	Erstellen Sie zusätzliche VMFS-Datenspeicher zum Hosten von virtuellen Maschinen für Microsoft SQL Server, Domain-Controller, vCenter Server und View Connection Server.	Speicher-Provisioning für VMFS-Datastores

Bereiten Sie das XtremIO-Array vor.

Diese Lösung macht keine bestimmten Einrichtungsschritte für das XtremIO-Array erforderlich. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung für das XtremIO-Array finden Sie in den folgenden Dokumenten:

- *EMC XtremIO-Speicherarray – Handbuch zur Vorbereitung des Aufstellorts*
- *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation*
- *EMC XtremIO-Speicherarray – Handbuch zur Softwareinstallation und Upgrade*
- *EMC XtremIO-Speicherarray – Handbuch zur Hardwareinstallation und Upgrade*

Vorbereiten des Isilon-Clusters

Diese Lösung macht keine bestimmten Einrichtungsschritte für das Isilon-Cluster erforderlich. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung für das Isilon-Cluster finden Sie in den folgenden Dokumenten:

- *X400 Installation Guide*
- *Leitfaden für Isilon-Standortplanung und -vorbereitung*

Bereiten Sie das VNX-Array vor.

Diese Lösung macht keine bestimmten Einrichtungsschritte für das VNX-Array erforderlich. Anweisungen für Zusammenstellung, Rackeinbau, Verkabelung und Stromversorgung für das VNX-Array finden Sie im relevanten VNX-Installationsleitfaden:

Konfigurieren des ersten XtremIO-Arrays

Nach der Vorbereitung des XtremIO-Arrays konfigurieren Sie die Schlüsselinformationen über die vorhandene Umgebung. Konfigurieren Sie Folgendes gemäß den für das Rechenzentrum Ihres Kunden geltenden Policies mit den Informationen der vorhandenen Infrastruktur.

- Domain Name System (DNS)
- Network Time Protocol (NTP)
- XMS-Netzwerkschnittstelle
- Schnittstellen des Speichernetzwerks
- IP-Adressen des Speichernetzwerks

Konfigurieren des ersten Isilon-Clusters

Nach der Vorbereitung des Isilon-Arrays konfigurieren Sie die Schlüsselinformationen über die vorhandene Umgebung. Konfigurieren Sie Folgendes gemäß den für das Rechenzentrum Ihres Kunden geltenden Policies mit den Informationen der vorhandenen Infrastruktur.

- Externe Netzwerkeinstellungen
- SmartConnect-Zonen
- Zugriffszonen

Weitere Informationen zur Konfiguration der Isilon-Plattform finden Sie in den in Kapitel 6 aufgelisteten Referenzdokumenten.

Konfigurieren des ersten VNX-Arrays

Nach der Vorbereitung des VNX-Arrays konfigurieren Sie die Schlüsselinformationen über die vorhandene Umgebung. Konfigurieren Sie Folgendes gemäß den für Ihr Rechenzentrum geltenden Policies mit den Informationen der vorhandenen Infrastruktur.

- DNS
- NTP
- Schnittstellen des Speichernetzwerks
- IP-Adresse des Speichernetzwerks
- CIFS-Services (Common Internet File System) und Microsoft Active Directory-Domainmitgliedschaft

Weitere Informationen zum Konfigurieren der VNX-Plattform finden Sie in den in Tabelle 8 auf Seite 17 aufgelisteten Referenzdokumenten. Informationen zum Laufwerkslayout finden Sie im Designleitfaden.

Speicher-Provisioning für VMFS-Datastores

Führen Sie das folgenden Verfahren aus, um Volumes auf dem XtremIO-Array zum Speichern der virtuellen Desktops zu konfigurieren:

1. Wählen Sie **Configuration** in der EMC XtremIO-Speichermanagementanwendung aus.
2. Klicken Sie unter **Volume** auf **Add**.
3. Klicken Sie im Fenster **Add New Volumes** auf **Add Multiple**.
4. Geben Sie unter **Number of Volumes** die erforderliche Anzahl der Datenspeicher ein, basierend auf den Konfigurationsdetails in Tabelle 9.

Tabelle 9. Volumes auf der XtremIO zum Speichern virtueller Desktops

Konfiguration	Anzahl Volumes	Größe des Volume (TB)
Virtuelle Desktops mit 1.250 vollständigen Clones	10	5
Virtuelle Desktops mit 1.750 verknüpften Clones	14	1
Virtuelle Desktops mit 2.500 vollständigen Clones	20	5
Virtuelle Desktops mit 3.500 verknüpften Clones	28	1



5. Geben Sie unter **Name** einen üblichen LUN-Namen ein.
6. Wählen Sie für **Size** je nach der Konfiguration entweder 1 TB oder 5 TB aus, wie in Tabelle 9 angegeben, und klicken Sie auf **OK**.

VNX FAST Cache konfigurieren

So zeigen Sie FAST Cache im VNX-Speicherpool für diese Lösung an und konfigurieren es:

1. Klicken Sie in Unisphere auf **Properties** und wählen Sie Manage Cache aus.
2. Wählen Sie **FAST-Cache** im Dialogfeld **Storage System Properties**, das in Abbildung 6 zu sehen ist.
3. So erstellen Sie FAST Cache:
   a. Klicken Sie auf **Create**, um das Dialogfeld Create FAST Cache zu öffnen.

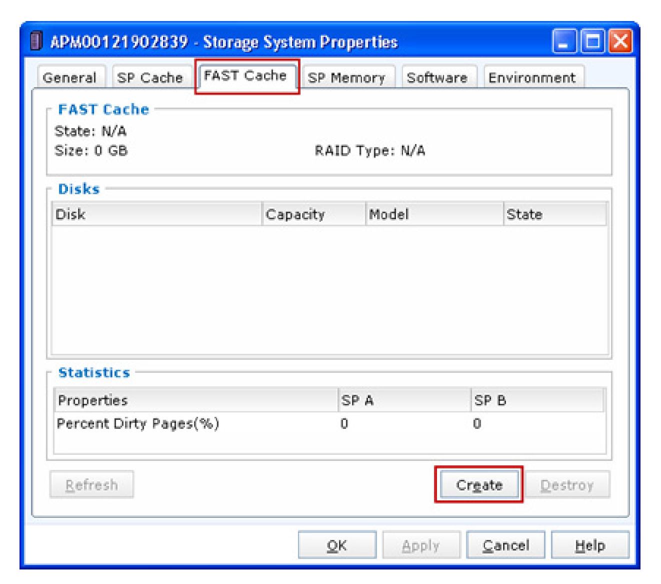


Abbildung 6. Dialogfeld

   b. Wählen Sie die erforderliche Anzahl der Laufwerke aus, die für FAST Cache verwendet werden sollen.

   Wenn Sie **Automatic** auswählen, wird im Dialogfeld eine Liste der Flash-Laufwerke angezeigt, die für das Erstellen von FAST-Cache verwendet werden.

   Mit der Option **Manual** können Sie die Laufwerke manuell auswählen.

   Um den RAID-Type auszuwählen, wählen Sie einen Wert aus der Drop-down-Liste aus, wie in Abbildung 7 dargestellt. Der Standardwert ist 1.

Hinweis: Wie Sie die Anzahl der zu verwendenden Festplatten festlegen, finden Sie in den Richtlinien im Designleitfaden.

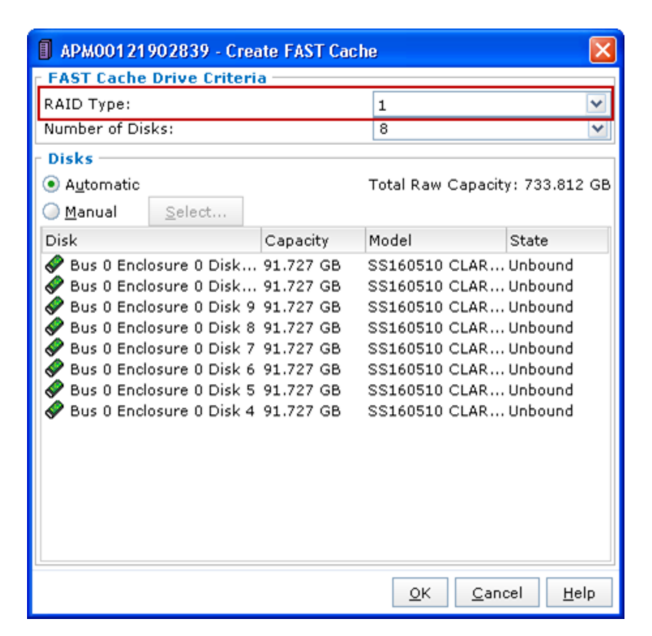


Abbildung 7. Dialogfeld

c. Klicken Sie auf **OK**, um den FAST Cache zu erstellen.

Hinweis: Wenn keine ausreichende Anzahl von Flash-Laufwerken verfügbar ist, wird eine Fehlermeldung angezeigt und FAST-Cache wird nicht erstellt.

Nachdem Sie FAST-Cache erstellt haben, ist es standardmäßig für alle Pools aktiviert, die nachfolgend erstellt werden.

d. Um FAST Cache für den vorhandenen Speicherpool, der für die Lösung erstellt wurde, zu aktivieren, wählen Sie **FAST Cache Enabled** unter **Advanced** im Dialogfeld **Storage Pool Properties**.

Die FAST Cache-Funktion auf VNX führt nicht zu einer sofortigen Performanceverbesserung. Das System muss Daten zu Zugriffsmustern sammeln und häufig verwendete Informationen in den Cache hochstufen. Dieser Prozess dauert einige Stunden, in denen sich die Performance des Arrays kontinuierlich verbessert.

Provisioning von optionalem Speicher für Benutzerdaten

Isilon

Gehen Sie folgendermaßen vor, um eine einzige, gemeinsame Share für kleine und mittlere Unternehmen (KMU) auf Isilon zu erstellen, die von allen Benutzern verwendet werden kann, was die einfachste Methode ist, eine Microsoft Windows-Umgebung einzurichten:

1. Klicken Sie in der OneFS-Webadministrationsoberfläche auf **Protocols › Windows Sharing (SMB)**.
2. Klicken Sie auf der Registerkarte **SMB Shares** auf **Add a share**.
3. Geben Sie in das Feld **Share Name** den Benutzernamen des Benutzers ein (z. B. Home-Verzeichnis).
4. Geben Sie in das Feld **Directory to Be Shared** den vollständigen Pfad des Home-Verzeichnisses ein, beginnend mit /ifs, oder klicken Sie auf **Browse**, um das Verzeichnis zu suchen (z. B. /ifs/home/).



5. Klicken Sie auf **Create**.

   In Abbildung 8 ist ein Beispiel für die Erstellung einer Share für KMUs dargestellt.

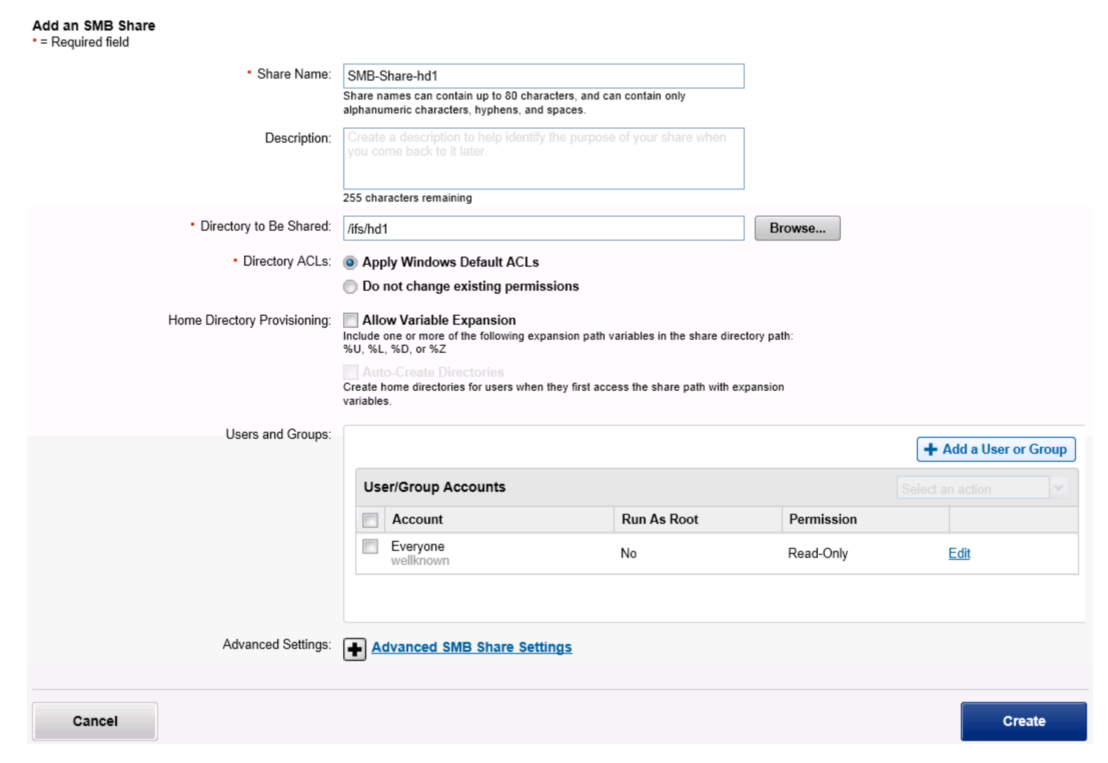


Abbildung 8. Erstellen einer KMU-Share auf Isilon

Standardmäßig haben alle Benutzer Zugriff auf die gemeinsame KMU-Share und können auf Dateien anderer Benutzer zugreifen, die ein Home-Verzeichnis in der KMU-Share haben. Wenn Sie strengere Zugriffsberechtigungen festlegen möchten, aktivieren Sie die Access-Based Enumeration-Funktion in Windows Server, um nur die Dateien und Ordner aufzuführen, auf die jeder Benutzer beim Durchsuchen der Inhalte auf dem Server Zugriff hat.

Informationen über andere Methoden der Konfiguration von Isilon als Home-Verzeichnis finden Sie unter *Managen von KMU-Shares und Benutzer-Home-Verzeichnissen in EMC Isilon OneFS 6.5 und höher.*

VNX

Wenn in der Produktionsumgebung noch kein für Benutzerdaten (das heißt Roamingbenutzerprofile oder View Persona Management Repositories und Stammverzeichnisse) erforderlicher Speicher vorhanden ist und die optionale Benutzerdatenspindel erworben wurde, führen Sie die folgenden Schritte in Unisphere aus, um 2 CIFS-Dateisysteme auf der VNX zu erstellen:

1. Erstellen Sie einen RAID-6-Speicherpool mit der in Tabelle 10 gezeigten Konfiguration.

Tabelle 10. Konfiguration für blockbasierte RAID-6-Speicherpools

Konfiguration	Anz. der Laufwerke	Drive type
1.250 virtuelle Desktops	16	2 TB NL-SAS
1.750 virtuelle Desktops	24	
2.500 virtuelle Desktops	40	
3.500 virtuelle Desktops	48	

Im Designleitfaden werden die Speicherlayouts beschrieben.

2. Stellen Sie die erforderlichen LUNs aus dem Pool zur Verfügung, wie in Tabelle 11 gezeigt, die dem Data Mover als Dvols eines systemdefinierten NAS-Pools angezeigt werden.

Tabelle 11. Konfigurieren von LUNs für NAS-Pools

Konfiguration	Anzahl der LUNs	LUN-Größe (TB)
1.250 virtuelle Desktops	10	1,5
1.750 virtuelle Desktops	10	2,25
2.500 virtuelle Desktops	10	3,75
3.500 virtuelle Desktops	20	2,25

3. Stellen Sie vier Dateisysteme aus dem NAS-Pool zum Exportieren als CIFS-Shares auf einem CIFS-Server bereit.

Konfigurieren von FAST VP für Benutzerdaten auf VNX (optional)

Optional können Sie FAST VP so konfigurieren, dass die Datenverschiebung zwischen Storage Tiers im Speicherpool für Benutzerdaten automatisiert wird. Sie können FAST VP auf Pool- oder LUN-Ebene konfigurieren.

Konfigurieren von FAST VP auf Poolebene

So konfigurieren Sie FAST VP auf der Poolebene:

1. Wählen Sie in Unisphere den Speicherpool für die Benutzerdaten aus und klicken Sie auf **Properties**.

2. Wählen Sie in **Storage Pool Properties** die Option **Tiering** aus, um die Tiering-Informationen für einen bestimmten Pool mit aktiviertem FAST VP anzuzeigen, wie in Abbildung 9 dargestellt.

   Tier Status zeigt FAST-VP-Verlagerungsinformationen an, die für den ausgewählten Pool spezifisch sind. **Tier Details** zeigt die genaue Verteilung der Daten an.



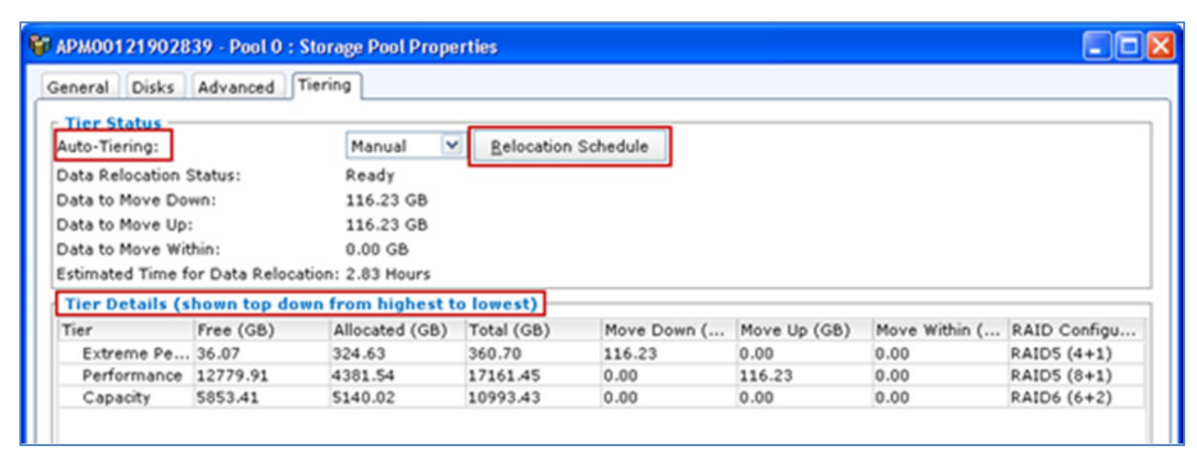


Abbildung 9. Dialogfeld

3. Sie können hier die Einstellung **Auto-Tiering** auf **Automatic** oder **Manual** setzen.

4. Um die geplante Verlagerung auf der Poolebene auszuwählen, klicken Sie auf **Relocation Schedule**, um das Dialogfeld **Manage Auto-Tiering** zu öffnen, wie in Abbildung 10 angezeigt.

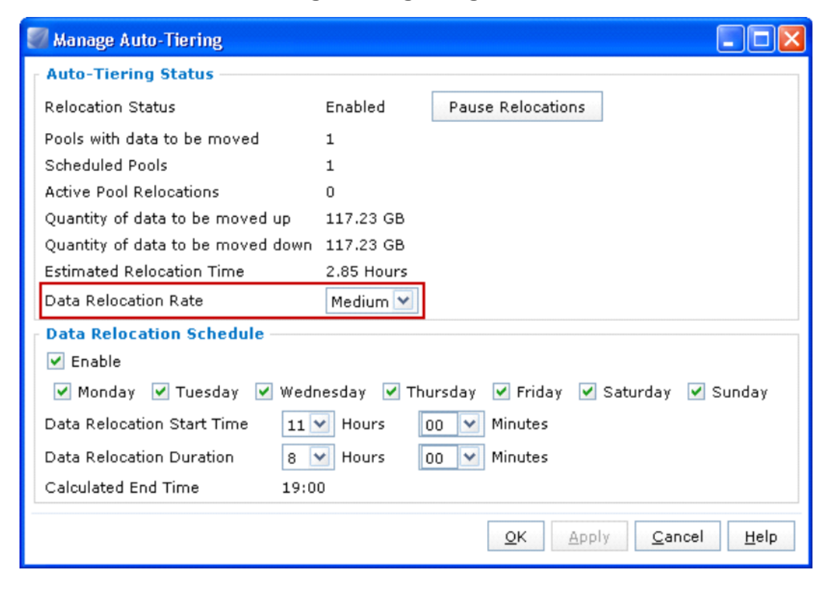


Abbildung 10. Dialogfeld Manage Auto-Tiering

Standardmäßig ist die **Data Relocation Rate** auf den Wert **Medium** eingestellt, sodass die Host-I/O-Vorgänge nicht wesentlich beeinträchtigt sind.

Hinweis: FAST VP ist ein vollständig automatisiertes Tool, bei dem Verlagerungen automatisch ausgeführt werden können. Sie sollten Verlagerungen außerhalb von Spitzenzeiten planen, um das Risiko von Performanceeinbußen zu minimieren.



VSPEX Private Cloud-Anforderungen:

Diese Proven Infrastructure für VSPEX-Anwender-Computing erfordert mehrere Anwendungsserver. Sofern nicht anders angegeben, verwenden alle Server Microsoft Windows Server 2012 R2 als Betriebssystem. In Tabelle 12 listet die Mindestanforderungen für jeden erforderlichen Infrastrukturserver auf.

Tabelle 12. Mindestanforderungen für den Infrastrukturserver

Server	CPU	RAM (GB)	IOPS	Speicherkapazität (GB)
Domain-Controller (je)	2 vCPUs	4	25	32
SQL Server	2 vCPUs	6	100	200
vCenter Server	4 vCPUs	8	100	80
View-Controller (je)	4 vCPUs	12	50	32

In den folgenden Dokumenten werden die Anforderungen für die optionalen Komponenten von vRealize Operations Manager für Horizon View und von VMware Workspace beschrieben:

- *VMware vRealize Operations Manager für Horizon View – Plattformprofil*
- *EMC VSPEX für VMware Workspace – Lösungsleitfaden*

Speicherlayout der Private Cloud

Diese Lösung benötigt die folgenden Volumes der angezeigten Größe für das Speichern der angegebenen virtuellen Maschinen:

- Ein 1-TB-Volume, um die virtuellen Maschinen des Infrastrukturservers zu hosten, die vCenter Server, View Connection Server, den Active Directory-Server und Microsoft SQL Server enthalten können.
- Für Konfigurationen für bis zu 1.750 Desktops: ein 1,8-TB-Volume, um die virtuelle Maschinen und Datenbanken mit vRealize Operations Manager für Horizon View zu hosten
- Für Konfigurationen für bis zu 3.500 Desktops: ein 3,6-TB-Volume, um die virtuelle Maschinen und Datenbanken mit vRealize Operations Manager für Horizon View zu hosten

Wenden Sie sich für weitere Informationen zu größeren Konfigurationen an Ihren EMC Vertriebsmitarbeiter.

Konfigurieren von XtremIO-Event Handler

Sie können XtremIO so konfigurieren, dass Ihnen Warnmeldungen per E-Mail zugesendet werden, wenn Events der Kategorie „Minor Cluster“ auftreten, z. B. Events, die mit clusterfreier Kapazität in Verbindung stehen. Das *EMC XtremIO-Speicherarray – Benutzerhandbuch* bietet eine vollständige Liste von XtremIO-Fehlern und -Warnmeldungen.

Wenn Sie einen Event-Handler erstellen möchten, um beim Auftreten dieser Events per E-Mail benachrichtigt zu werden, gehen Sie folgendermaßen vor:

1. Wählen Sie in der XtremIO-Speichermanagementanwendung **Alerts & Events** aus der Menüleiste aus.
2. Klicken Sie im Fenster **Alerts & Events** auf **Events**.
3. Klicken Sie auf das Symbol **Display Event Handlers**, wie in Abbildung 11 dargestellt.



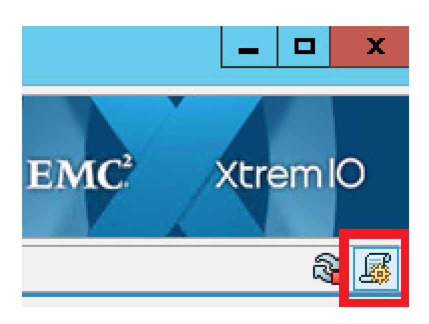


Abbildung 11. XtremIO-Symbolschaltfläche „Display Event Handlers“

4. Klicken Sie im Fenster **Event Handlers** auf **Add**.
5. Wählen Sie im Dialogfeld **Add Event Handler**, wie in Abbildung 12 angezeigt, Folgendes aus, wobei sich Cluster auf den Namen des XtremIO-Clusters bezieht, das bei der Installation angegeben wurde:
   - **Kategorie**: Software
   - **Schweregrad**: Minor
   - **Entität**: Cluster
   - **Details zur Entität**: Clustername
6. Wählen Sie im selben Dialogfeld **Send email** aus und klicken Sie dann auf **OK**.

   Sie können die Warnmeldung auch konfigurieren, indem Sie **Send SNMP Trap** oder **Send to Syslog** auswählen.

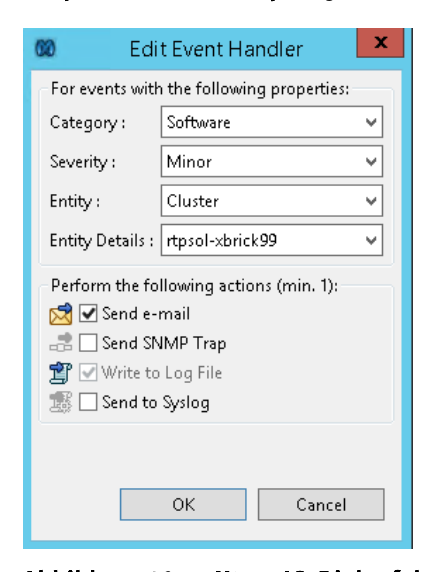


Abbildung 12. XtremIO-Dialogfeld „Edit Event Handler“

7. Wählen Sie **Administration** in der Menüleiste aus.
8. Klicken Sie unter **Administration** - **Email Configuration** auf Add, um alle E-Mail-Adressen hinzuzufügen, die Kopien von XtremIO-Warnmeldungen erhalten sollen.

   Wenn Sie den Event Handler so konfiguriert haben, dass Warnmeldungen entweder mit SNMP oder Syslog versendet werden, müssen Sie diese Optionen je nach Bedarf in **SNMP Configuration** oder in **Syslog Configuration** entsprechend konfigurieren.

Installieren und Konfigurieren der vSphere-Hosts

In diesem Abschnitt finden Sie Informationen zur Installation und Konfiguration der vSphere-Hosts und Infrastrukturserver, die zur Unterstützung der Architektur erforderlich sind. In Tabelle 13 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Tabelle 13. Aufgaben für die Serverinstallation

Aufgabe	Beschreibung	Referenz
Installieren von vSphere	Installieren Sie den vSphere-Hypervisor auf den physischen Servern, die für die Lösung bereitgestellt werden.	*Installations- und Einrichtungshandbuch für VMware vSphere*
Konfigurieren des vSphere-Netzwerks	Konfigurieren Sie das vSphere-Netzwerk, einschließlich NIC-Trunking (Netzwerkschnittstellenkarten), VMkernel-Ports und virtuellen Maschinenportgruppen.	• VMware vSphere-Netzwerkdokumentation • Konfigurieren des vSphere-Netzwerks
Hinzufügen von vSphere-Hosts zu XtremIO-Initiatorgruppen	Fügen Sie die vSphere-Hosts den Initiatorgruppen hinzu, die in Vorbereiten und Konfigurieren der Speicherarray erstellt wurden.	*VMware vSphere – Installations- und Einrichtungshandbuch*
Verbinden der VMware-Datenspeicher	Verbinden Sie die VMware-Datastores mit den für die Lösung bereitgestellten vSphere-Hosts.	• *Handbuch für vSphere-Speicher* • vSphere-Datastores anschließen
vSphere optimieren:	Nehmen Sie die erforderlichen Änderungen an der Konfiguration vor, um eine optimale Performance des XtremIO-Arrays sicherzustellen	• *EMC XtremIO-Speicherarray – Benutzerhandbuch* • vSphere für XtremIO optimieren

Installieren von vSphere

Bestätigen oder aktivieren Sie nach dem ersten Einschalten der für vSphere verwendeten Server im BIOS jedes Servers die Einstellung für die hardwaregestützte CPU-Virtualisierung und die hardwaregestützte MMU-Virtualisierung. Wenn die Server mit einem RAID-Controller ausgestattet sind, empfiehlt EMC, eine Spiegelung auf den lokalen Festplatten zu konfigurieren.

Installieren Sie mithilfe der vSphere-Installationsmedien den Hypervisor auf jedem der Server. Für die Installation sind vSphere-Hostnamen, IP-Adressen und ein Root-Passwort erforderlich. In Arbeitsblatt für die Kundenkonfiguration finden Sie die entsprechenden Werte.

Konfigurieren des vSphere-Netzwerks

Der *VMware* vSphere-Netzwerkleitfaden beschreibt die vSphere-Netzwerkkonfiguration, einschließlich Lastenausgleich, Linkzusammenfassung und Failover-Optionen. Wählen Sie die entsprechende Option für den Lastenausgleich auf der Basis dessen aus, was von der Netzwerkinfrastruktur unterstützt wird. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.



Netzwerkschnittstellenkarten

Während der Installation von vSphere wird ein virtueller Standardswitch (vSwitch) erstellt. Standardmäßig wählt vSphere nur eine physische NIC als virtuellen Switch-Uplink aus. Zum Erfüllen der Redundanz- und Bandbreitenanforderungen konfigurieren Sie eine zusätzliche NIC, entweder über die vSphere-Konsole oder durch eine Verbindung mit dem vSphere-Host vom vSphere-Client aus.

Jeder vSphere-Server sollte über mehrere NICs für jedes virtuelle Netzwerk verfügen, um Redundanz und die Verwendung von Netzwerklastenausgleich, Link-Zusammenfassung und Netzwerkadapter-Failover zu ermöglichen.

VMKernel-Ports

Erstellen Sie VMkernel-Ports nach Bedarf, basierend auf der Infrastrukturkonfiguration:

- VMkernel-Port für vMotion
- Virtuelle Desktopportgruppen (verwendet von den virtuellen Desktops für die Kommunikation im Netzwerk)

Im *VMware vSphere-Netzwerkleitfaden* wird das Verfahren für die Konfiguration dieser Einstellungen beschrieben. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

vSphere-Datastores anschließen

Verbinden Sie die in Vorbereiten und Konfigurieren der Speicherarrays konfigurierten Datenspeicher mit den entsprechenden vSphere-Servern. Dazu zählen die Datastores, die für die folgenden Zwecke konfiguriert wurden:

- Virtueller Desktopspeicher
- Virtueller Infrastrukturmaschinenspeicher (falls erforderlich)
- SQL Server-Speicher (falls erforderlich)

Um vSphere-Servern den Zugriff auf XtremIO-Volumes zu gestatten, konfigurieren Sie die XtremIO-Initiatorgruppen und fügen Sie die entsprechenden vSphere-Hosts jeder Gruppe folgendermaßen hinzu:

1. Wählen Sie **Configuration** in der XtremIO-Storage Management-Anwendung aus.
2. Klicken Sie in **Inititator Group** auf **Add**.
3. Geben Sie im Dialogfeld **Add New Initiator Group** einen Namen im Feld **Initiator Group Name** ein und klicken Sie dann auf **Add**.
4. Geben Sie im Dialogfeld **Add Initiator** einen Namen in das Feld **Initiator Name** ein und wählen Sie dann im Listenfeld **Initiator Port Address** den Initiatorport eines vSphere-Servers aus, der in der Zielinitiatorgruppe sein sollte.
5. Klicken Sie auf **OK**, um zum Dialogfeld **Add Initiator** zurückzukehren.
6. Wiederholen Sie die Schritte 4 und 5 nach Bedarf, um alle Zielinitiatorports zu der Initiatorgruppe hinzuzufügen, und klicken Sie dann auf **Finish**, wenn Sie alle Initiatoren hinzugefügt haben.
7. Wählen Sie in **Configuration** die Ziel-Volumes in **Volumes** aus, wählen Sie die Zielinitiatorgruppe in **Initiator Groups** aus, klicken Sie auf **Map All** und klicken Sie dann auf **Apply**, um den Prozess abzuschließen und den Serverzugriff auf die ausgewählten Volumes zu gewähren.



8. Wiederholen Sie bei Bedarf den vorherigen Schritt, um den verbleibenden Initiatorgruppen Zugriff auf die verbleibenden Volumes zu gewähren.
9. Führen Sie den Vorgang **Rescan for Datastores** auf den vSphere-Hosts durch, damit die Hosts sofort Zugriff die XtremIO-Volumes haben, für die ihnen Zugriff gewährt wurde.
10. Wiederholen Sie dieses Verfahren nach Bedarf, um eine Initiatorgruppe für jeden vSphere-Cluster zu erstellen.

Der *VMware vSphere-Speicherleitfaden* enthält Anweisungen zur Formatierung der vSphere-Datenspeicher, sobald XtremIO-Initiatorgruppen konfiguriert wurden. Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

vSphere für XtremIO optimieren

Sie müssen mehrere Änderungen an den vSphere-Einstellungen vornehmen, um eine optimale Performance des XtremIO-Arrays sicherzustellen, wenn es mit vSphere verwendet wird.

Hinweis: Die Einstellungen, die in diesem Abschnitt beschrieben werden, gelten nur für vSphere-Hosts, die mit XtremIO-Arrays verbunden sind, und sollten nicht auf Block-Datastores angewendet werden, die auf anderen Arrays, einschließlich anderer EMC Arrays, gehostet werden. Diese Einstellungen können Sie auf vSphere-Hosts anwenden, die mit NFS-Datastores und XtremIO verbunden sind. Diese Einstellungen haben keine Auswirkung auf die Kommunikation mit diesen NFS-Datastores.

Folgende Änderungen, beschrieben in dem *EMC XtremIO-Speicherarray – Benutzerhandbuch*, sind erforderlich:

- Ändern Sie die vSphere-Speichergerätpfadauswahl zu **Round Robin (VMware)** für jeden vSphere-Datenspeicher. Sie können diese Änderung mithilfe des folgenden vSphere-PowerCLI-Befehls für jedes Cluster ausführen, indem Sie anstelle von *cluster* den Namen des vSphere-Clusters eintragen, in dem sich die Ziel-vSphere-Hosts befinden.

```
Get-VMHost -location cluster | get-scsilun -luntype "disk"
| where {$_.MultipathPolicy -ne "RoundRobin"} | Set-ScsiLun
-MultipathPolicy "RoundRobin"
```

- Ändern Sie die vSphere-Einstellung **Disk.SchedQuantum** in **64** und die Einstellung **Disk.DiskMaxIOSize** in **4096**. Sie können diese Änderungen durch Ausführen der folgenden vSphere-PowerCLI-Befehle für jedes Cluster vornehmen, indem Sie anstelle von *cluster* den Namen des vSphere-Clusters eintragen, in dem sich die Ziel-vSphere-Hosts befinden:

```
Get-VMhost -location cluster | Set-
VMhostAdvancedConfiguration Disk.SchedQuantum -Value 64
Get-VMhost -location cluster | Set-
VMhostAdvancedConfiguration Disk.DiskMaxIOSize -Value 4096
```

- Ändern Sie die vSphere-Einstellung **Disk.SchedNumReqOutstanding** für jeden vSphere-Datenspeicher in **256**. Sie können diese Änderung vornehmen, indem Sie das folgende vSphere PowerCLI-Skript für jedes Cluster ausführen, wobei Sie anstelle von *ClusterName* den Namen des Zielclusters eintragen:

```
$vmhosts = get-vmhost –location ClusterName
foreach ($vmhost in $vmhosts) {
$esxcli = get-esxcli -vmhost $vmhost
```




```
$AllLUNs = get-scsilun -vmhost $vmhost | where {$_.vendor -
eq "XtremIO"}
foreach ($lun in $AllLUNs) {
$CN = $lun.canonicalname
$EsxCli.storage.core.device.set($null, $cn, $null, $null,
$null, $null, $null, 256, $on)
}
}
```

4.4 EMC Virtual Storage Integrator

Das EMC Virtual Storage Integrator (VSI)-Plug-in ermöglicht Administratoren das Ausführen der häufigsten XtremIO-Administrationsaufgaben auf dem vSphere Web Client, anstelle die XtremIO-Managementkonsole nutzen zu müssen. Außerdem können Administratoren das Plug-in zum Ausführen von wichtigen Optimierungen am vSphere-Host für XtremIO verwenden, anstatt vSphere PowerCLI nutzen zu müssen. Wenn ein VNX-Array als Teil dieser Lösung bereitgestellt wird, können Administratoren das VSI-Plug-in auch zum Managen des VNX-Speichers nutzen.

Wenn Ihre Lösung das VSI-Plug-in verwendet, finden Sie im *EMC VSI für VMware vSphere Web Client – Produktleitfaden* Anweisungen für die Installation, Konfiguration und den Betrieb.

In Abbildung 13 wird eine EMC VSI-Installation dargestellt, die in den vSphere Web Client integriert wurde, wie auf der Seite **vCenter Home** angezeigt.

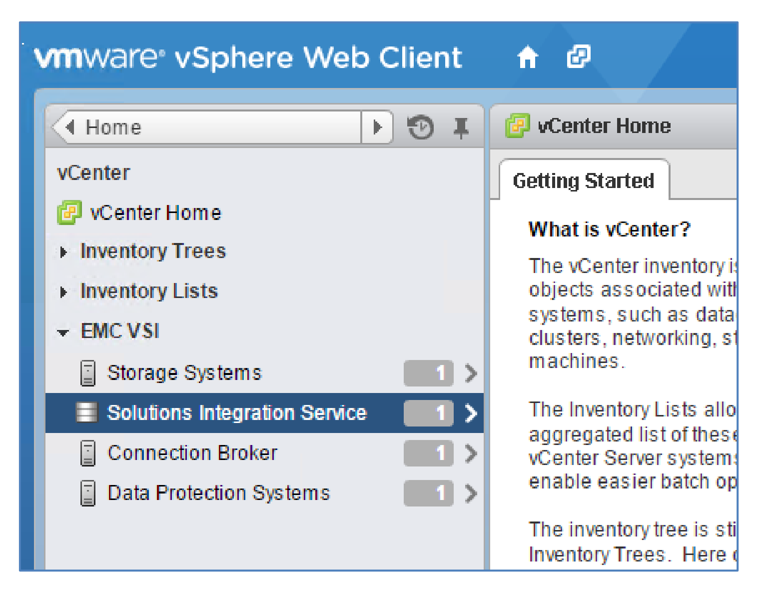


Abbildung 13. vSphere Web Client EMC VSI-Integration

Unter der Option **vCenter Home** › **Storage Systems** werden alle EMC Speichersysteme aufgeführt, nachdem Sie die dem VSI-Plug-in hinzugefügt haben. In dem Beispiel in Abbildung 14 wurde das XtremIO-Array hinzugefügt und ist für das Management im vSphere Web Client verfügbar.

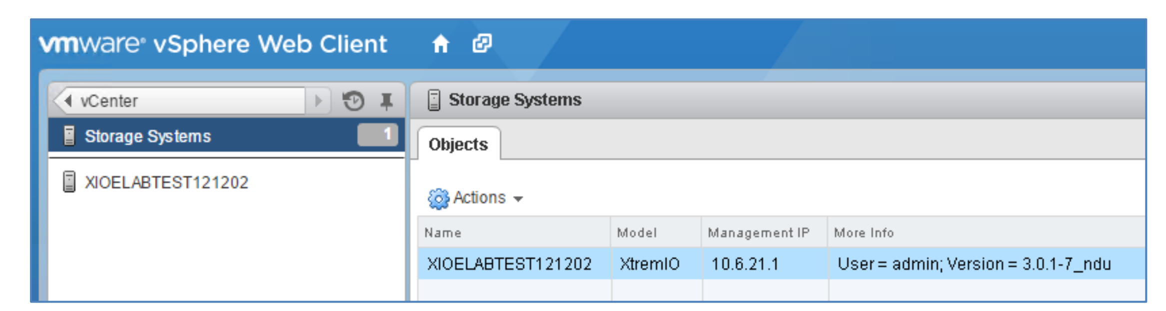


Abbildung 14. vSphere Web Client EMC VSI – Speichersysteme

Wenn Sie ein Array zum VSI-Plug-in hinzugefügt haben, listet der vSphere Web Client alle Datenspeicher des Arrays auf. Klicken Sie mit der rechten Maustaste auf einen Datenspeicher und wählen Sie **All EMC VSI Plugin Actions** aus, um auf alle Aktionen zuzugreifen, die Sie auf diesen Datenspeicher anwenden können, wie in Abbildung 15 dargestellt.

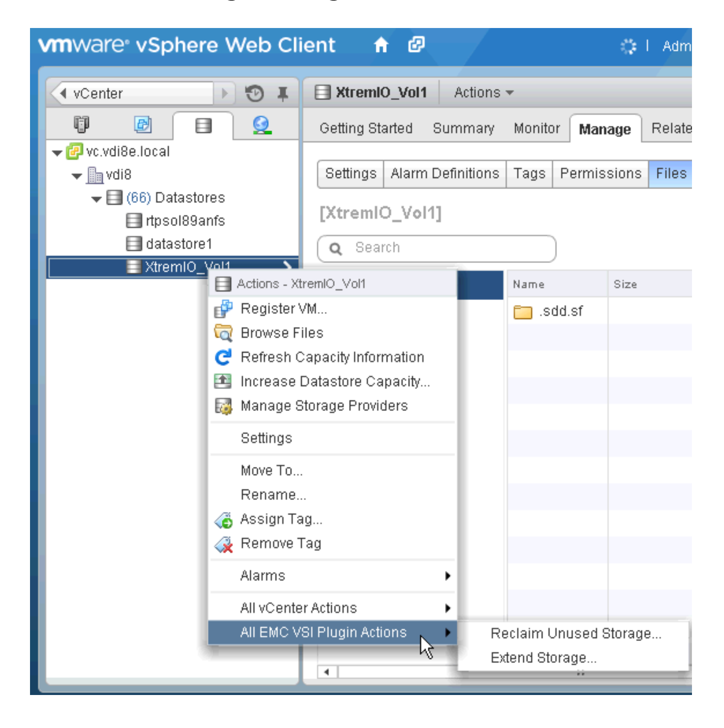


Abbildung 15. vSphere Web Client EMC VSI XtremIO-Datenspeicheraktionen

Optimieren der vSphere-Hosts für XtremIO

Sie müssen mehrere vSphere-Hosteinstellungen aktualisieren, um eine optimale Performance des XtremIO-Arrays mit vSphere sicherzustellen. Im *EMC XtremIO-Speicherarray – Benutzerhandbuch* sind diese Einstellungen umrissen.

Sie können die erforderlichen Einstellungen mit einer der folgenden Methoden implementieren:

- EMC VSI-Plug-in
- vSphere PowerCLI-Skripte

Beide Optionen erzielen dieselben Ergebnisse. Das EMC VSI-Plug-in bietet jedoch die schnellste und einfachste Methode, die erforderlichen Einstellungen zu implementieren. Die PowerCLI-Skripte automatisieren den Prozess und sind in Umgebungen nützlich, in denen die automatisierte Implementierung der Einstellungen besonders bevorzugt ist.

Wenn die XtremIO-Volumes bereits für die vSphere-Hosts bereitgestellt wurden, müssen Sie das EMC VSI-Plug-in anstelle der PowerCLI-Skripte zum Implementieren der Einstellungen verwenden.

Hinweis: Die Einstellungen gelten nur für vSphere-Hosts, die mit XtremIO-Arrays verbunden sind. Wenden Sie sie nicht auf Block-Datenspeicher an, die auf anderen Arraytypen gehostet werden, einschließlich anderen EMC Arrays. Sie können die Einstellungen jedoch auf vSphere-Hosts anwenden, die mit NFS-Datenspeichern verbunden sind, da die Einstellungen keine Auswirkung auf die Kommunikation mit diesen NFS-Datenspeichern haben.



Optimieren der vSphere- und XtremIO-Performance mithilfe des EMC VSI-Plug-in

Gehen Sie folgendermaßen vor, um die Optimierungseinstellungen mit dem EMC VSI-Plug-in zu konfigurieren:

1. Melden Sie sich bei dem vSphere Web Client mit einem Konto an, das Administratorrechte für vSphere und das EMC VSI-Plug-in hat.
2. Navigieren Sie zum Fenster **Hosts and Clusters**.
3. Klicken Sie in der Liste der vSphere-Hosts mit der rechten Maustaste auf einen Host, der die aktualisierten Einstellungen erfordert, und wählen Sie **All EMC VSI Plugin Actions** › **ESX Host Settings** aus, wie in Abbildung 16 dargestellt.

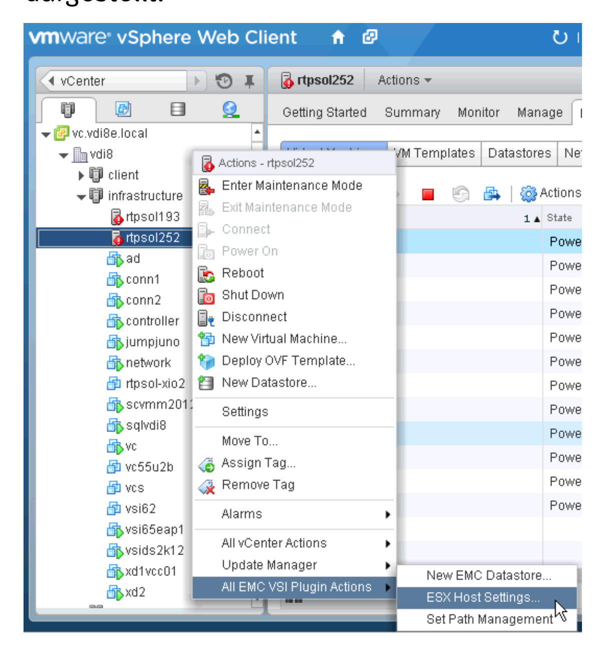


Abbildung 16. vSphere Web Client EMC VSI-Hosteinstellungen

4. Wählen Sie für **Set Host Settings** alle verfügbaren Optionen aus, wie in Abbildung 17 dargestellt, und klicken Sie dann auf **Next**.

Hinweis: Secure Shell (SSH)-Zugriff auf den vSphere-Host ist erforderlich und ein Neustart ist für die Implementierung aller Einstellungen erforderlich.

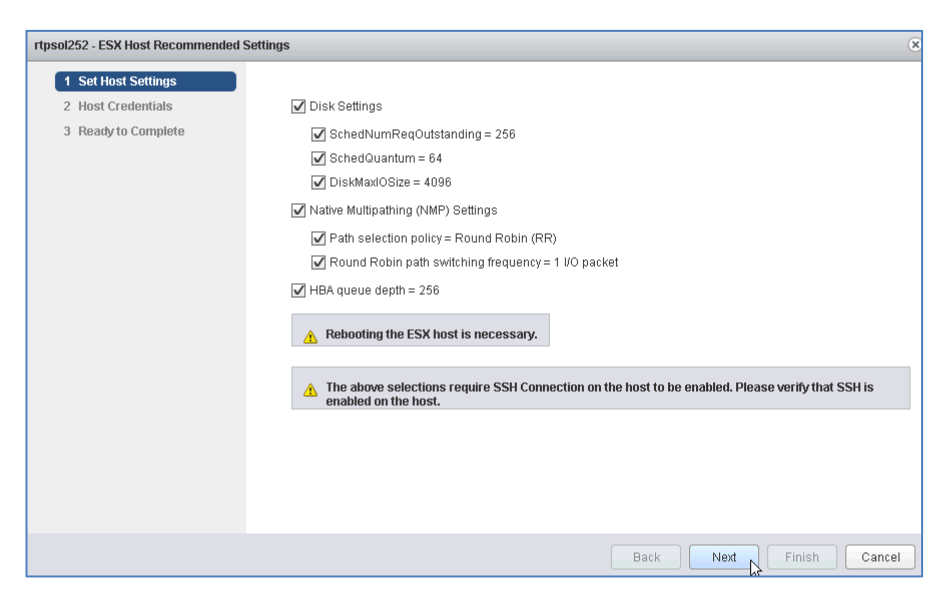


Abbildung 17. vSphere Web Client EMC VSI: Festlegen der Hosteinstellungen

5. Geben Sie unter **Host Credentials** die Anmeldedaten für ein lokales Konto auf dem vSphere-Host ein und klicken Sie auf **Next**.

Hinweis: Das lokale Konto muss über Root-Zugriff verfügen.

6. Prüfen Sie unter **Ready to Complete** die vorgeschlagenen Änderungen und klicken Sie dann auf **Finish**.
7. Wiederholen Sie die Schritte 3 – 6 für die anderen vSphere-Hosts im Cluster.

Die vSphere-Hosts sind jetzt mit den optimalen Einstellungen für die Verwendung mit XtremIO konfiguriert.

Installieren und Konfigurieren der SQL Server-Datenbank

In Tabelle 14 beschreibt die Aufgaben für die Einrichtung und Konfiguration einer Microsoft SQL Server-Datenbank für die Lösung. Wenn die Aufgaben abgeschlossen sind, ist SQL Server auf einer virtuellen Maschine eingerichtet und alle für vCenter, VMware vSphere Update Manager, Horizon View und View Composer erforderlichen Datenbanken sind für die Verwendung konfiguriert.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle SQL Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. In Tabelle 12 auf Seite 38 werden die empfohlenen Werte für CPU und Arbeitsspeicher dargestellt.



Tabelle 14. Aufgaben für die SQL Server-Datenbankkonfiguration

Aufgabe	Beschreibung	Referenz
Erstellen einer virtuellen Maschine für Microsoft SQL Server	Erstellen Sie eine virtuelle Maschine zum Hosten von SQL Server auf einem der vSphere-Server, der für virtuelle Infrastrukturmaschinen vorgesehen ist, und verwenden Sie den für die gemeinsame Infrastruktur bestimmten Datastore. Überprüfen Sie, ob der virtuelle Server die Hardware- und Softwareanforderungen erfüllt.	*VMware vSphere für virtuelle Maschinen – Administratorhandbuch*
Installieren von Microsoft Windows auf der virtuellen Maschine	Installieren Sie Microsoft Windows Server 2012 R2 Standard Edition auf der virtuellen Maschine.	Installieren und Bereitstellen von Windows Server 2012 R2
Installieren von Microsoft SQL Server	Installieren Sie Microsoft SQL Server 2012 auf der virtuellen Maschine.	SQL Server-Installation (SQL Server 2012)
Konfigurieren der Datenbank für vCenter Server	Erstellen Sie die für vCenter Server erforderliche Datenbank auf dem entsprechenden Datastore.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der Datenbank für vSphere Update Manager	Erstellen Sie die für vSphere Update Manager erforderliche Datenbank auf dem entsprechenden Datenspeicher.	*Vorbereiten der Update Manager-Datenbank*
Konfigurieren der Datenbank für View Composer	Erstellen Sie die für View Composer erforderliche Datenbank auf dem entsprechenden Datenspeicher.	*VMware Horizon View – Installationshandbuch*
Konfigurieren der Datenbank für View Manager	Erstellen Sie die für die View Manager-Ereignisprotokolle erforderliche Datenbank auf dem entsprechenden Datenspeicher.	
Konfigurieren der Datenbankberechtigungen für Horizon View und View Composer	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für die Horizon View- und View Composer-Datenbanken.	*VMware Horizon View – Installationshandbuch*
Konfigurieren der vCenter-Datenbank-berechtigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für vCenter.	*Vorbereiten der vCenter Server-Datenbanken*
Konfigurieren der vSphere Update Manager-Datenbank-berechtigungen	Konfigurieren Sie den Datenbankserver mit den entsprechenden Berechtigungen für vSphere Update Manager.	*Vorbereiten der Update Manager-Datenbank*



Bereitstellen von VMware vCenter Server

In Tabelle 15 beschreibt die Aufgaben zur Konfiguration von VMware vCenter Server für die Lösung.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für die virtuelle vCenter Server-Maschine in den Pool der VSPEX Private Cloud zu integrieren. In Tabelle 12 auf Seite 38 werden die empfohlenen Werte für CPU und Arbeitsspeicher dargestellt.

Tabelle 15. Aufgaben für die vCenter-Konfiguration

Aufgabe	Beschreibung	Referenz
Erstellen der virtuellen vCenter-Hostmaschine	Erstellen Sie eine virtuelle Maschine für vCenter Server.	*VMware vSphere für virtuelle Maschinen – Administratorhandbuch*
Installieren des vCenter-Gastbetriebssystems	Installieren Sie Windows Server 2012 R2 Standard Edition auf der virtuellen vCenter-Hostmaschine.	VMware vSphere-Dokumentation
Aktualisieren der virtuellen Maschine	Installieren Sie VMware Tools, aktivieren Sie die Hardwarebeschleunigung und den Remotezugriff auf die Konsole.	*vSphere für virtuelle Maschinen – Administratorhandbuch*
Erstellen von vSphere Update Manager ODBC-Verbindungen	Erstellen Sie die 64-Bit- und 32-Bit-vSphere Update Manager ODBC-Verbindungen.	• *VMware vSphere – Installations- und Einrichtungshandbuch* • *Installieren und Verwalten von VMware vSphere Update Manager*
Installieren von vCenter Server	Installieren Sie die vCenter Server-Software.	*Installations- und Einrichtungshandbuch für VMware vSphere*
Installieren von vSphere Update Manager	Installieren Sie die vSphere Update Manager-Software.	*Installieren und Verwalten von VMware vSphere Update Manager*
Erstellen des virtuellen Rechenzentrums	Erstellen Sie ein virtuelles Rechenzentrum.	*Handbuch für VMware vCenter Server- und Hostverwaltung*
Anwenden der vSphere-Lizenzschlüssel	Geben Sie die vSphere-Lizenzschlüssel in das vCenter-Lizenzierungsmenü ein.	*Installations- und Einrichtungshandbuch für VMware vSphere*
Hinzufügen von vSphere-Hosts	Verbinden Sie den vCenter-Server mit den vSphere-Hosts.	*VMware vCenter Server- und Hostverwaltung – Handbuch*
Konfigurieren von vSphere-Clustering	Erstellen Sie ein vSphere-Cluster und verschieben Sie die vSphere-Hosts in das Cluster.	*VMware vSphere-Ressourcenverwaltung – Handbuch*

Aufgabe	Beschreibung	Referenz
Installieren des vSphere Update Manager-Plug-ins	Installieren Sie das vSphere Update Manager-Plug-in von der Administrationskonsole.	*Installieren und Verwalten von VMware vSphere Update Manager*
Bereitstellen von EMC PowerPath/VE	Stellen Sie mithilfe von vSphere Update Manager das PowerPath/VE-Plug-in für alle vSphere-Hosts bereit.	*Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
Installieren von EMC VSI für VMware vSphere-Plug-in	Installieren Sie VSI für VMware vSphere-Plug-in auf der Administrationskonsole.	*EMC VSI für VMware vSphere: Unified Storage Management – Produktleitfaden*
EMC PowerPath Viewer installieren	Installieren Sie PowerPath Viewer auf der Administrationskonsole.	*PowerPath Viewer – Installations- und Administrationshandbuch*

Einrichten von View Connection Server

In diesem Abschnitt finden Sie Informationen zum Einrichten und Konfigurieren von View Connection Server für die Lösung. Für eine Neuinstallation von Horizon View empfiehlt VMware, dass Sie die folgenden Aufgaben in der in Tabelle 16 angegebenen Reihenfolge durchführen.

Hinweis: EMC empfiehlt, die Betriebssystem-Volumes für die virtuellen View Connection Server-Maschinen in den Pool der VSPEX Private Cloud zu integrieren. In Tabelle 12 auf Seite 38 werden die empfohlenen Werte für CPU und Arbeitsspeicher dargestellt.

Tabelle 16. Aufgaben für die Einrichtung von View Connection Server

Aufgabe	Beschreibung	Referenz
Erstellen virtueller Maschinen für View Connection Server	Erstellen Sie zwei virtuelle Maschinen in vSphere Client. Diese virtuellen Maschinen werden als View Connection Server-Hosts verwendet. Installieren Sie Windows Server 2012 R2 als Gastbetriebssystem für diese Server.	*VMware Horizon View – Installationshandbuch*
Installieren von View Connection Server	Installieren Sie die View Connection Server-Software auf einer der zuvor vorbereiteten virtuellen Maschinen. Geben Sie den Horizon View-Lizenzschlüssel in die VMware View Manager-Administrationskonsole ein.	VMware Horizon View-Dokumentaktion

Aufgabe	Beschreibung	Referenz
Konfigurieren der Verbindung zur Horizon View-Ereignisprotokolldatenbank	Konfigurieren Sie die Einstellungen für die Horizon View-Ereignisprotokolldatenbank mithilfe der entsprechenden Datenbankinformationen und Anmeldedaten.	
Hinzufügen einer Replikatinstanz von View Connection Server	Installieren Sie die View Connection Server-Software auf dem zweiten Server.	
Konfigurieren der View Composer-ODBC-Verbindung	Konfigurieren Sie entweder auf dem vCenter Server oder einem dedizierten Windows Server 2012 R2-Server eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank.	
Installieren von View Composer	Installieren Sie View Composer auf dem im vorherigen Schritt verwendeten Server.	
Verbinden von Horizon View mit vCenter und View Composer	Verbinden Sie Horizon View über die VMware View Manager-Webbenutzeroberfläche mit dem vCenter Server und View Composer.	*VMware Horizon View – Administratorhandbuch*
Vorbereiten einer virtuellen Master-Maschine	Erstellen Sie eine virtuelle Master-Maschine als Basis-Image für die virtuellen Desktops.	
Konfigurieren von View Persona Management-Gruppen-Policies	Konfigurieren Sie Active Directory-Gruppen-Policies, um View Persona Management zu aktivieren.	
Konfigurieren der Gruppen-Policies für die Ordnerumleitung für Avamar	Konfigurieren Sie Active Directory-Gruppen-Policies, um die Ordnerumleitung für Avamar zu aktivieren.	
Konfigurieren von Horizon View PCoIP-Gruppen-Policies	Konfigurieren Sie Active Directory-Gruppen-Policies für PCoIP-Protokolleinstellungen.	

Installieren von View Connection Server

Installieren Sie die View Connection Server-Software gemäß den Anweisungen im *VMware Horizon View – Installationshandbuch*. Wählen Sie **Standard** aus, wenn Sie aufgefordert werden, den **View Connection Server** einzugeben. Geben Sie den Horizon View-Lizenzschlüssel in die View Manager-Webkonsole ein.



Konfigurieren der Verbindung zur Horizon View-Ereignisprotokolldatenbank

Konfigurieren Sie die Verbindung zur Horizon View-Ereignisprotokolldatenbank mithilfe des Datenbankservernamens, des Datenbanknamens und der Datenbankanmeldedaten. Spezifische Informationen zum Konfigurieren des Ereignisprotokolls finden Sie in *VMware Horizon View – Installationshandbuch*.

Hinzufügen einer Replikatinstanz von View Connection Server

Wiederholen Sie den Installationsprozess für den View Connection Server auf der zweiten virtuellen Zielmaschine. Wenn Sie aufgefordert werden, den Verbindungsservertyp einzugeben, geben Sie **Replica** an, und stellen Sie dann die Horizon View-Administrator-Anmeldedaten bereit, um die Horizon View-Konfigurationsdaten der ersten Horizon View Connection Server-Instanz zu replizieren.

Konfigurieren der View Composer-ODBC-Verbindung

Erstellen Sie auf dem Server, der den View Composer-Service hostet, eine ODBC-Verbindung für die zuvor konfigurierte View Composer-Datenbank. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie in *VMware Horizon View – Installationshandbuch*.

Installieren von View Composer

Installieren Sie die View Composer-Software auf dem Server, der den View Composer-Service hostet. Geben Sie auf Aufforderung während des Installationsprozesses die zuvor konfigurierte ODBC-Verbindung an. Spezifische Informationen zum Konfigurieren der ODBC-Verbindung finden Sie in *VMware Horizon View – Installationshandbuch*.

Verbinden von Horizon View mit vCenter und View Composer

Erstellen Sie mithilfe der VMware View Manager-Webkonsole die Verbindung zwischen Horizon View und dem vCenter Server und View Composer. Spezifische Informationen zum Erstellen der Verbindungen finden Sie in *VMware Horizon View – Administratorhandbuch*. Wenn die Option zur Aktivierung von vSphere-Host-Caching (auch als Horizon View Storage Accelerator oder Content Based Read Cache bezeichnet) Verfügung gestellt wird, aktivieren Sie die Option und legen Sie die Cachegröße auf 2 GB fest, welches die maximal unterstützte Größe ist.

Sie können darüber hinaus die Option **Reclaim VM** disk space aktivieren. Wenn Sie **Reclaim VM disk space** aktivieren, müssen Sie einen Blackout-Zeitraum festlegen, während dessen der Vorgang nicht ausgeführt wird. Da der Vorgang nicht zu Spitzenzeiten ausgeführt werden sollte, muss der Blackout-Zeitraum diese Zeiten abdecken. Standardmäßig wird die Speicherplatzrückgewinnung erst dann ausgeführt, wenn mindestens 1 GB zurückgewonnen werden kann. Sie können einen anderen Wert beim Implementieren der Desktop-Pools festlegen.

Vorbereiten einer virtuellen Master-Maschine

So bereiten Sie die virtuelle Mastermaschine vor:

1. Erstellen Sie mithilfe des vSphere Web Client eine virtuelle Maschine auf Grundlage der Hardwarespezifikationen für VMware Version 9.

   Sie können virtuelle Maschinen mit Version 9 nicht mit dem vSphere Client erstellen. Verwenden Sie dazu den vSphere Web Client.

2. Installieren Sie Windows 7 oder Windows 8.1 als Gastbetriebssystem.
3. Installieren Sie entsprechende Integrationstools wie VMware Tools.
4. Optimieren Sie die Betriebssystemeinstellungen, um zu verhindern, dass unnötige Hintergrundservices irrelevante I/O-Vorgänge generieren, die sich negativ auf die allgemeine Performance des Speicherarrays auswirken.

Detaillierte Informationen finden Sie im *Optimierungshandbuch für Windows 7 und Windows 8 für VMware Horizon View.*

5. Installieren Sie Drittanbietertools oder -anwendungen wie Microsoft Office, die für Ihre Umgebung relevant sind.
6. Installieren Sie die Avamar Desktop/Laptop-Clientsoftware.
7. Details finden Sie im *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX für Anwender-Computing mit VMware Horizon View*
8. Installieren Sie den Horizon View-Agent.

Hinweis: Wenn Sie die Horizon View Persona Management-Funktion verwenden, installieren Sie zu diesem Zeitpunkt die Persona Management-Komponente des Horizon View-Agent. Achten Sie darauf, dass die Persona Management-Option während der Installation des Horizon View-Agent ausgewählt wird.

---

9. Installieren Sie den VMware Workspace-Agent (optional; nur erforderlich, wenn auf VMware Workspace über Horizon View-Desktops zugegriffen wird).
10. Wenn Sie Desktops mit vollständigen Clones bereitstellen, erstellen Sie eine vSphere Customization Specification, die für die Desktopanpassung verwendet wird.

    Anweisungen zum Erstellen und Managen von Anpassungsspezfikationen finden Sie im VMware-Dokument *vSphere-VM – Administratorhandbuch*. Dieser Schritt ist nicht erforderlich, wenn Sie Desktops mit verknüpften Clones bereitstellen.

Konfigurieren von Horizon View Persona Management-Gruppen-Policies

View Persona Management wird über Active Directory-Gruppen-Policies aktiviert, die der Organisationseinheit zugewiesen werden, die die Computerkonten für den virtuellen Desktop enthält. Die Vorlagen für die View-Gruppen-Policy befinden sich im Verzeichnis **\Program Files\VMware\VMware Horizon View\Server\extras\GroupPolicyFiles** auf dem View Connection-Server.

Konfigurieren der Gruppen-Policies für die Ordnerumleitung für Avamar

Aktivieren Sie die Ordnerumleitung über die Active Directory-Gruppen-Policies, die der Organisationseinheit zugewiesen werden, die die Benutzerkonten für den virtuellen Desktop enthält. Die Active Directory-Ordnerumleitung wird (statt der View Persona Management-Ordnerumleitung) verwendet, damit für die Ordner die von der Avamar-Software geforderten Benennungskonsistenzen beibehalten werden. Detaillierte Informationen finden Sie unter *EMC Backup und Recovery für VSPEX für Anwender-Computing für VMware Horizon View*.

Konfigurieren von Horizon View PCoIP-Gruppen-Policies

Horizon View PCoIP-Protokolleinstellungen werden über Active Directory-Gruppen-Policies gesteuert, die den Organisationseinheiten zugewiesen werden, die die Horizon View Connection-Server enthalten. Die Vorlagen für die View-Gruppen-Policy befinden sich auf dem View-Verbindungsserver im Verzeichnis **\Program Files\VMware\VMware View\Server\extras\GroupPolicyFiles**. Verwenden Sie die Gruppen-Policy-Vorlage **pcoip.adm**, um die folgenden PCoIP-Protokolleinstellungen festzulegen:

- **Maximum Initial Image Quality value**: 70
- **Maximum Frame Rate value**: 24



- **Build-to-Lossless deaktivieren:** Aktiviert

Hinweis: Höhere Bildraten für die PCoIP-Sitzung und eine höhere Bildqualität können sich nachteilig auf die Serverressourcen auswirken.

Provisioning von virtuellen Desktops mit View Composer

Stellen Sie mithilfe der View Manager-Administrationskonsole Ihre virtuellen Desktops folgendermaßen bereit:

1. Erstellen Sie einen **Automated Desktop Pool**.
2. Geben Sie den bevorzugten Wert für die **User Assignment**-Methode an:
   - **Dedicated**: Benutzer erhalten bei jeder Anmeldung beim Pool denselben Desktop. Diese Methode wird in der Regel bei Desktops mit vollständigen Clones verwendet.
   - **Floating**: Benutzer erhalten bei jeder Anmeldung zufällig aus dem Pool ausgewählte Desktops.
3. Klicken Sie auf **Weiter**.
4. Legen Sie **View Composer linked clones** oder **Full virtual machines** (vollständige Clones) fest und klicken Sie auf **Next**.
5. Legen Sie einen Wert für die Desktop-Pool-**ID** fest und klicken Sie auf **Next**.
6. Konfigurieren Sie **Desktop Pool Settings** nach Bedarf und klicken Sie auf **Next**.
7. Konfigurieren Sie **Provisioning Settings** nach Bedarf und klicken Sie auf **Next**.
8. Wenn Sie einen Pool von verknüpften Clones erstellen, akzeptieren Sie die Standardwerte für **View Composer Disks** oder bearbeiten Sie die Werte nach Bedarf.

   Dieser Schritt wird nicht angezeigt, wenn Sie einen Pool mit vollständigen virtuellen Maschinen erstellen.

9. Wenn **View Persona Management** verwendet wird, wählen Sie **Do not redirect Windows profile** im Bereich **Persistent Disk** aus (siehe Abbildung 18).

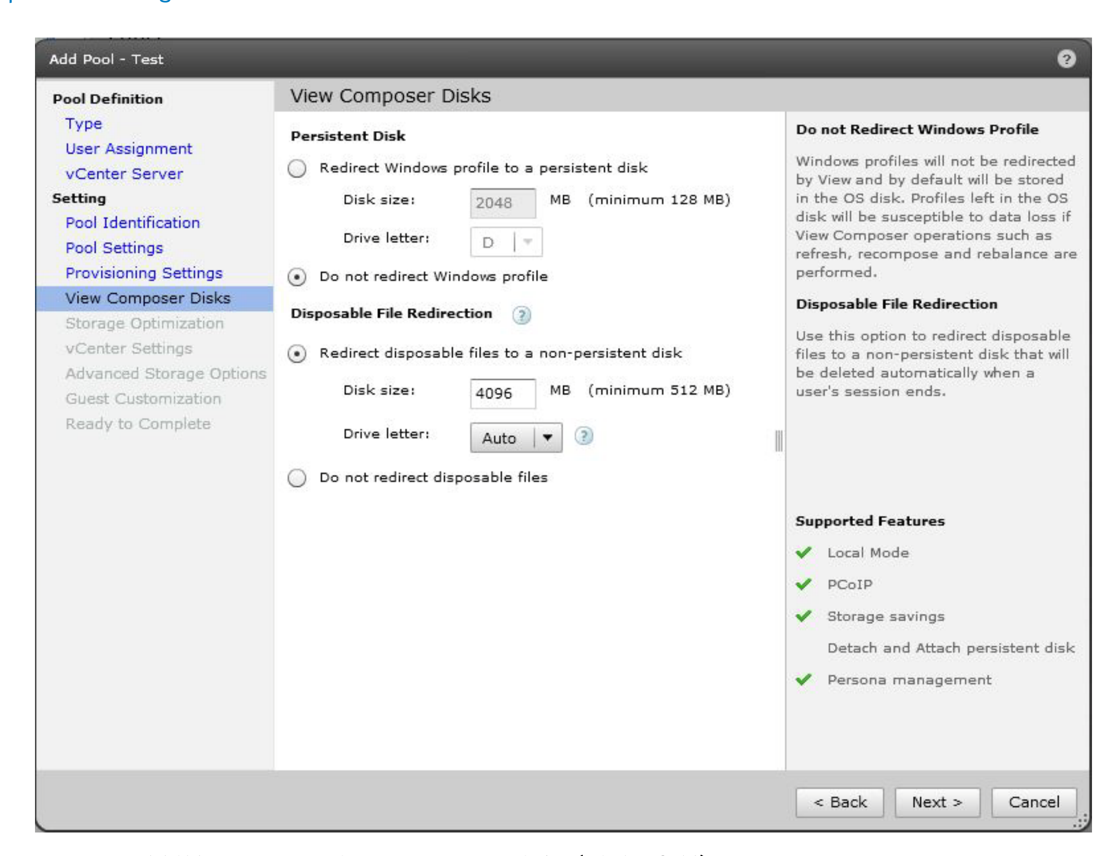


Abbildung 18. View Composer Disks (Dialogfeld)

10. Klicken Sie auf **Weiter**.

    Das Dialogfeld **Storage Optimization** wird angezeigt. Es sind keine Änderungen erforderlich.

11. Klicken Sie auf **Weiter**.

12. Wenn Sie einen Pool verknüpfter Clones für View Composer bereitstellen, wählen Sie die entsprechende übergeordnete virtuelle Maschine, den Snapshot der virtuellen Maschine, den Ordner, den vSphere-Host oder die vSphere-Cluster, den vSphere-Ressourcenpool sowie die Datenspeicher aus.

    Wenn Sie einen Pool mit vollständigen virtuellen Maschinen bereitstellen, wählen Sie die entsprechende virtuelle Maschinenvorlage, den Ordner, den vSphere-Host oder das vSphere-Cluster, den vSphere-Ressourcenpool sowie die Datenspeicher aus.

13. Klicken Sie auf **Weiter**.

14. Aktivieren Sie optional **Use View Storage Accelerator** für den Desktoppool und geben Sie Blackoutzeiten für die Cacheregeneration an.

    Wenn Sie einen Pool verknüpfter Clones für View Composer bereitstellen, können Sie außerdem **Reclaim VM disk space** aktivieren und **Blackout Times** festlegen.

15. Legen Sie Image-Anpassungsoptionen nach Bedarf fest und wählen Sie entweder **Use QuickPrep** für Pools verknüpfter Clones unter View Composer oder **Use a customization specification (Sysprep)** für Pools vollständiger virtueller Maschinen (vollständiger Clones) aus.

16. Schließen Sie den Poolerstellungsprozess ab, um die Erstellung des virtuellen Desktoppools zu initiieren.



17. Wenn View Persona Management verwendet werden soll, konfigurieren Sie es mithilfe der Anweisungen im *Horizont View – Installationshandbuch*.

Provisioning von virtuellen Desktops mit VSI

Stellen Sie mithilfe von EMC Virtual Storage Integrator (VSI) für VMware vSphere Web Client virtuelle Desktops mit vollständigen Clones bereit, indem Sie diese folgendermaßen einem neuen Pool hinzufügen.

Hinweis: Sie können die virtuellen Desktops auch für einen vorhandenen Pool bereitstellen. Informationen zum Provisioning von virtuellen Desktops für einen vorhandenen Pool und detaillierte Informationen zum Einrichten der VSI-Umgebung finden Sie im *EMC VSI für VMware vSphere Web Client – Produktleitfaden*.

---

1. Melden Sie sich beim VMware vSphere Web Client an.
2. Klicken Sie mit der rechten Maustaste auf die virtuelle Maschine des Master-Image und wählen Sie **All EMC VSI Plugin Actions** › **EMC Clone**.
3. Geben Sie im Feld **Select base name and folder** einen Namen für den Clone ein, wählen Sie den Zielordner aus und klicken Sie dann auf **Next**.
4. Wählen Sie im Listenfeld **Select a compute resource** ein Cluster, einen Host, eine vApp oder einen Ressourcenpool aus, auf dem oder der die virtuellen Maschinen-Clones ausgeführt werden sollen, und klicken Sie dann auf **Next**.
5. Geben Sie für die **Select clone**-Optionen die folgenden Informationen an:
   - **Clone count**: Geben Sie die Anzahl der Clones ein, die Sie erstellen möchten.
   - **Generated clone name**:
     – **Add leading zeros to index used to generate names**: Wählen Sie diese Option aus, um den Indexzahlen in den Dateinamen führende Nullen hinzuzufügen.
     – **Number of digits in index**: Geben Sie die Gesamtanzahl der Ziffern ein, die am Ende des Clone-Namens angehängt werden soll.
   - **Customization specification**: Eine Liste aller benutzerdefinierten Ziele vom Anpassungsspezifikations-Manager.
   - **Select destination datastore**: Wählen Sie einen vorhandenen XtremIO-Datenspeicher aus oder wählen Sie **New**, um einen neuen Zieldatenspeicher für die Clones zu erstellen.
   - **Power on virtual machines after creation**: Wählen Sie diese Option aus, um den virtuellen Maschinen-Clone automatisch einzuschalten.
6. Wählen Sie unter **Connection Broker Information** die Option **Integrate with VMware View** und klicken Sie auf **Next**.
7. Wählen Sie für **Pool Choice** einen VMware View Server aus der Liste aus, wählen Sie **Add VMs to a new Pool** und klicken Sie auf **Next**.
8. Geben Sie für **Pool Name** eine eindeutige ID, einen Anzeigenamen und eine optionale Beschreibung in die entsprechenden Felder ein und wählen Sie eine Option für **Desktop Persistence**.

9. Wählen Sie für **Pool Settings** die gewünschten Werte für die folgenden Optionen aus:
    - **Wenn die VM nicht verwendet wird**
    - **Automatische Abmeldung nach Trennung**
    - **Benutzern das Rücksetzen ihres Desktops erlauben**
    - **Standardanzeigeprotokoll**
    - **Adobe Flash-Qualität**
    - **Adobe Flash-Drosselung**
10. Überprüfen Sie im Fenster **Ready to Complete** die Einstellungen und klicken Sie auf **Finish**.

Rückgewinnen von physischer XtremIO-Kapazität

vSphere markiert nicht automatisch Blöcke als verfügbar, nachdem ihr Inhalt gelöscht wurde. Um nicht verwendeten Speicherplatz wieder in das XtremIO-Array für die zukünftige Nutzung zurückzuführen, müssen Sie einen SCSI UNMAP-Vorgang für jeden vSphere-Datenspeicher im Fenster für die Rechenzentrumswartung durchführen.

Sie können einen SCSI UNMAP-Vorgang über eine der folgenden Methoden ausführen:

- Führen Sie mithilfe eines Skripts den Befehl **esxcli storage vmfs unmap** auf einem der vSphere-Hosts aus, der mit dem Zieldatenspeicher verbunden ist. Der Befehl ist in vSphere 5.5 und höher verfügbar und hervorragend für Umgebungen geeignet, in denen die Automatisierung des SCSI UNMAP-Prozesses bevorzugt ist.
- Führen Sie mithilfe des EMC VSI-Plug-in schnell den Vorgang in dem vSphere Web Client durch. Für diese Methode ist es erforderlich, dass das EMC VSI-Plug-in in der vSphere-Umgebung installiert und konfiguriert ist und mit dem XtremIO-Zielarray verbunden.

Bei beiden Methoden wird dasselbe Ergebnis erzielt, wählen Sie also die Methode aus, die am besten in Ihre regelmäßige vSphere-Wartungsvorgänge passt. Weitere Informationen über den SCSI UNMAP-Vorgang finden Sie im VMware Knowledgebase-Artikel *Using esxcli in vSphere 5.5 to reclaim VMFS deleted blocks on thin-provisioned LUNs (2057513)*.

Überlegungen zum SCSI UNMAP-Vorgang

Ein SCSI UNMAP-Vorgang erfordert ungefähr 20 Prozent freien Speicherplatz im vSphere-Datenspeicher. Wenn der Datenspeicher nicht über ausreichend freien Speicherplatz verfügt, wird die Kapazität während des SCSI UNMAP-Vorgangs aufgefüllt und die vSphere-Hosts erhalten in der Regel Simple Traversal of User Datagram Protocol Through Network Address Translators (STUN)-Anforderungen von einer oder mehreren der virtuellen Maschinen im Datenspeicher, bis der Speicherplatz frei ist.



SCSI UNMAP-Vorgänge sind I/O-intensiv. Sie sollten diese Vorgänge in Zeiten durchführen, in denen das XtremIO-Array nicht stark ausgelastet ist, um die Wahrscheinlichkeit zu mindern, dass Mandanten mit im Array gehosteten Desktops eine Verschlechterung der Performance spüren. Wenn die physische Kapazität des Arrays jedoch niedrig ist, führen Sie den SCSI UNMAP-Vorgang sofort aus, ohne Rücksicht auf die aktuelle I/O-Last.

Durchführen von SCSI UNMAP-Vorgängen mithilfe eines Skripts

Um ungenutzte Speicherblöcke mit dem Befehl **esxcli** zurückzugewinnen, führen Sie den Befehl auf einem vSphere-Host aus, der mit dem Zieldatenspeicher verbunden ist. Sie können den Befehl entweder in einer SSH-Sitzung mit dem vSphere-Host oder über eine vSphere Management Assistant (vMA)-Sitzung ausführen, die eine Verbindung mit dem Host herstellt.

Geben Sie den folgenden Befehl ein, wobei *vSphereDatastoreName* für den Namen des Datenspeichers steht, für den Sie den SCSI UNMAP-Vorgang durchführen möchten:

```
esxcli storage vmfs unmap -l vSphereDatastoreName -n 20000
```

Der Befehl erzeugt keine Ausgabe und im Bereich **Recent Tasks** im vSphere Web Client werden keine Statusinformationen für den Befehl angezeigt. Sie können aber folgendermaßen den Bandbreitenverlauf entweder in der XtremIO-Speichermanagementanwendung oder in der EMC Storage Analytics (ESA)-Benutzeroberfläche anzeigen, um zu prüfen, ob der Vorgang abgeschlossen ist:

- Wählen Sie in der XtremIO-Speichermanagementanwendung **Dashboard** › **Performance** › **Bandwidth** aus.
- Wählen Sie in der ESA-Benutzeroberfläche **Storage Metrics** › **Metric Picker** › **Total Bandwidth** aus.

Wie in Abbildung 19 und Abbildung 20 dargestellt, können Sie die Auswirkung des SCSI UNMAP-Vorgangs ganz einfach an der merkbaren Erhöhung der Bandbreite während der Ausführung des Befehls erkennen.

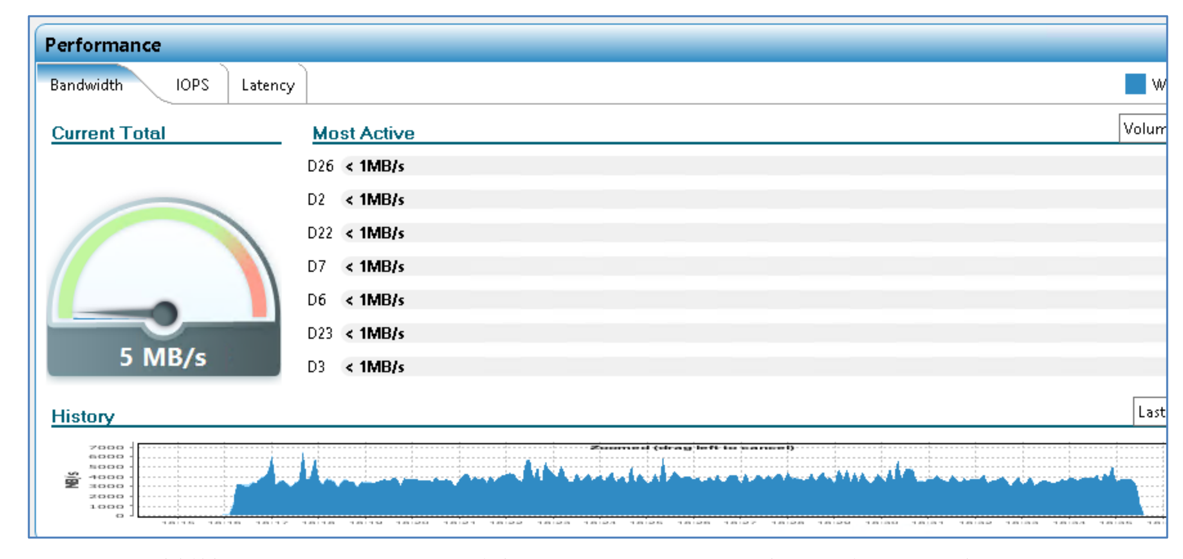


Abbildung 19. XtremIO-Speichermanagementanwendung: Diagramm der Performancebandbreite

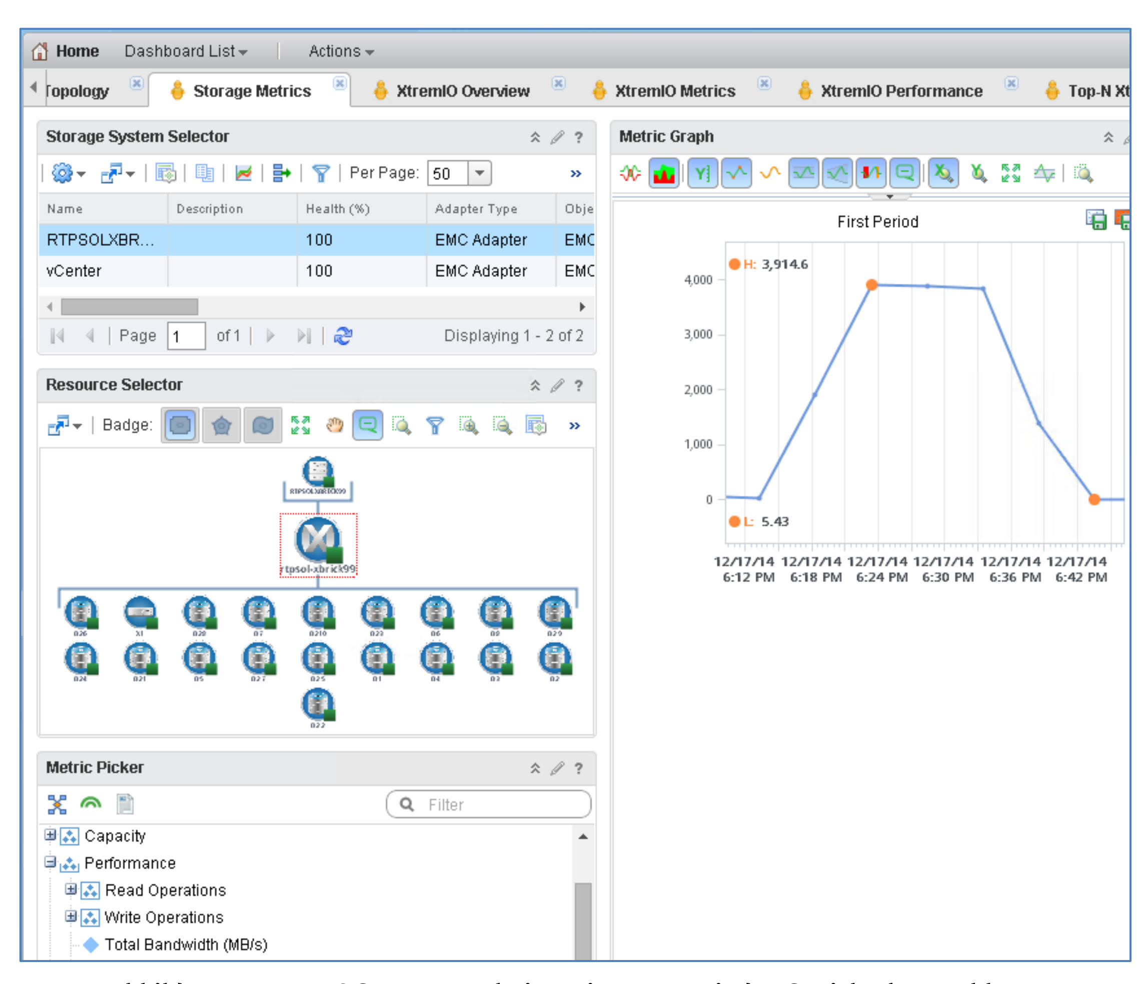


Abbildung 20. EMC Storage Analytics: Diagramm mit den Speicherkennzahlen

Durchführen von SCSI UNMAP-Vorgängen mithilfe von EMC VSI

Wenn Ihre Lösung das EMC VSI-Plug-in nutzt, können Sie einen SCSI UNMAP-Vorgang schnell auf dem vSphere Web Client ausführen, indem Sie folgendermaßen vorgehen:

1. Klicken Sie im vSphere Web Client auf der Seite **Home** auf das Symbol **Storage**.
2. Klicken Sie mit der rechten Maustaste auf den XtremIO-Zieldatenspeicher für den SCSI UNMAP-Vorgang und wählen Sie **All EMC VSI Plugin Actions** › **Reclaim Unused Storage**, wie in Abbildung 21 dargestellt.



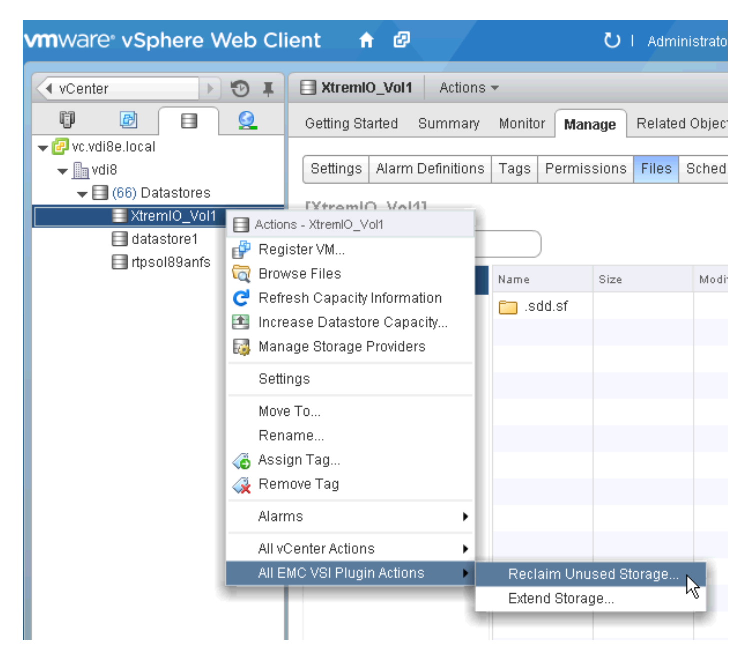


Abbildung 21. vSphere Web Client EMC VSI-Rückgewinnung von ungenutztem Speicher

3. Geben Sie unter **Reclamation Details** den Benutzernamen und das Passwort eines lokalen Kontos auf dem ausgewählten vSphere-Host ein und klicken Sie dann auf **Next**.

Hinweis: Das lokale Konto muss über Root-Zugriff verfügen.

EMC VSI wählt automatisch einen Host aus, der zum Durchführen des SCSI UNMAP-Vorgangs verwendet werden soll, wie in Abbildung 22 dargestellt.

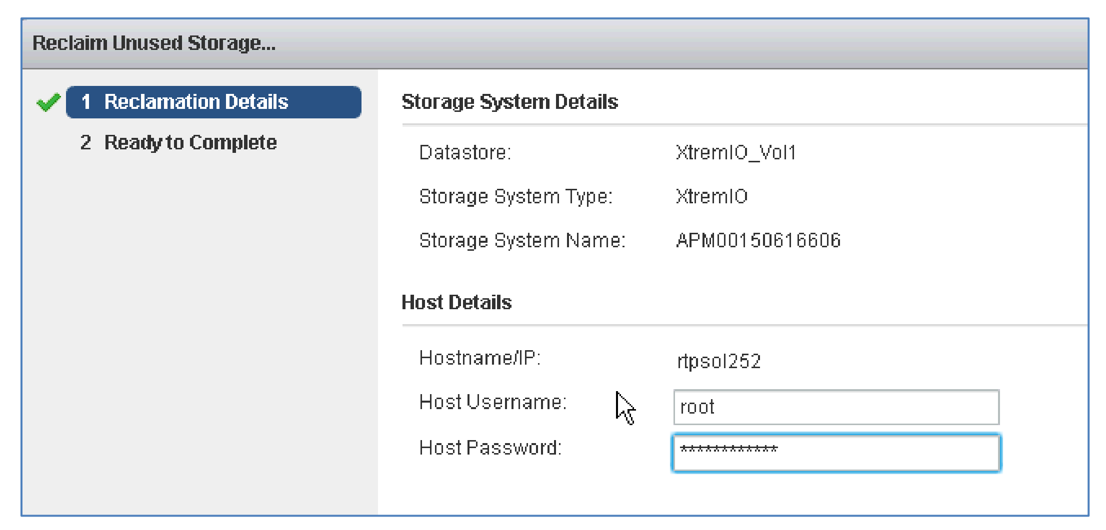


Abbildung 22. vSphere Web Client Reclamation Details

4. Prüfen Sie unter **Ready to Complete** die Details für den SCSI UNMAP-Vorgang und klicken Sie dann auf **Finish**.

5. Wählen Sie **Recent Tasks › Running**, um den Status des SCSI UNMAP-Vorgangs anzuzeigen, wie in Abbildung 23 dargestellt.

Sie können den Status des Vorgangs auch prüfen, indem Sie die Bandbreitenstatistiken des XtremIO-Arrays anzeigen, wie unter Durchführen von SCSI UNMAP-Vorgängen mithilfe eines Skripts beschrieben.

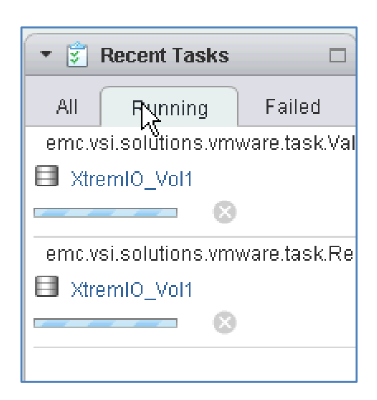


Abbildung 23. vSphere Web Client Ausführen einer Ansicht unter „Recent Tasks“

Einrichten von EMC Avamar Backup und Recovery

Wenn Ihre Lösung Avamar Backup und Recovery umfasst, finden Sie detaillierte Informationen zur Implementierung der Backup- und Recovery-Lösung im *Design- und Implementierungsleitfaden: EMC Backup und Recovery für VSPEX für Anwender-Computing für VMware Horizon View*.

Einrichten von VMware vShield Endpoint

In diesem Abschnitt werden Informationen zum Einrichten und Konfigurieren der Komponenten von VMware vShield Endpoint bereitgestellt. In Tabelle 17 beschreibt die Aufgaben, die abgeschlossen werden müssen.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für vShield Endpoint in den Pool der VSPEX Private Cloud zu integrieren. Weitere Informationen zur empfohlenen CPU- und Arbeitsspeicherkonfiguration finden Sie in *VMware vShield – Kurzanleitung*.

Tabelle 17. Für die Installation und Konfiguration von vShield Endpoint erforderliche Aufgaben

Aufgabe	Beschreibung	Referenz
Überprüfen der Desktoptreiberinstallation für vShield Endpoint	Überprüfen Sie, ob die vShield Endpoint-Treiberkomponente von VMware Tools auf dem virtuellen Desktop Master Image installiert wurde.	*VMware vShield – Kurzanleitung*
Bereitstellen der vShield Manager-Appliance	Führen Sie die Bereitstellung und Konfiguration der vShield Manager-Appliance durch.	
Registrieren des vShield Manager-Plug-Ins	Registrieren Sie das vShield Manager-Plug-in beim vSphere-Client.	



Aufgabe	Beschreibung	Referenz
Anwenden von vShield Endpoint-Lizenzen	Wenden Sie die vShield Endpoint-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an.	
Installieren des vShield Endpoint-Services	Installieren Sie den vShield Endpoint-Service auf den vSphere-Desktop-Hosts.	
Bereitstellen eines Managementservers für die Virenschutzlösung	Führen Sie die Bereitstellung und Konfiguration eines Managementservers für die Virenschutzlösung durch.	*VMware vShield – Kurzanleitung* **Hinweis**: Die Management-Serversoftware für die Virenschutzlösung und virtuellen Sicherheitsmaschinen werden von vShield Endpoint-Partnern bereitgestellt. Genaue Details zur Installation und Konfiguration finden Sie in der Dokumentation des Anbieters.
Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen	Führen Sie die Bereitstellung und Konfiguration der virtuellen Sicherheitsmaschinen (SVMs) auf jedem vSphere-Desktophost durch.	
Überprüfen der vShield Endpoint-Funktion	Überprüfen Sie die Funktion der vShield Endpoint-Komponenten mithilfe des virtuellen Desktop Master Image.	**Hinweis**: Details zur Überprüfung der vShield Endpoint-Integration und -Funktion finden Sie in der Dokumentation des Anbieters.

Überprüfen der Desktoptreiberinstallation für vShield Endpoint

Der vShield Endpoint-Treiber ist eine Subkomponente des VMware Tools-Softwarepakets, das auf dem virtuellen Desktop Master Image installiert ist. Installieren Sie den Treiber mithilfe einer der folgenden Methoden:

- Wählen Sie während der VMware Tools-Installation **Complete** aus.
- Wählen Sie während der VMware Tools-Installation **Custom** aus. Wählen Sie im Listenfeld **VMware Device Drivers VMCI Driver** und dann vShield Driver aus.

Zum Installieren des vShield Endpoint-Treibers auf einer virtuellen Maschine, auf der VMware Tools bereits installiert sind, initiieren Sie die VMware Tools-Installation, und wählen Sie die entsprechende Option aus.

Bereitstellen der vShield Manager-Appliance

Die vShield Manager-Appliance wird von VMware als OVA-Datei bereitgestellt, die über den vShield-Client mithilfe von **File > Deploy OVF template** importiert wird. Die vShield Manager-Appliance ist mit allen erforderlichen Komponenten vorkonfiguriert.

Installieren des vShield Endpoint-Services

Der vShield Endpoint-Service muss auf allen virtuellen vSphere-Desktophosts installiert sein. Der Service wird auf den vSphere-Hosts von der vShield Manager-Appliance installiert. Verwenden Sie die vShield Manager-Webkonsole für die Initiierung der vShield Endpoint-Serviceinstallation und zur Überprüfung der erfolgreichen Installation.

Bereitstellen eines Managementservers für die Virenschutzlösung

Der Managementserver für die Virenschutzlösung wird für das Management der Virenschutzlösung verwendet und von vShield Endpoint-Partnern bereitgestellt. Der Managementserver und damit verbundene Komponenten sind eine erforderliche Komponente der vShield Endpoint-Plattform.

Bereitstellen der virtuellen vSphere-Sicherheitsmaschinen

Die virtuellen vSphere-Sicherheitsmaschinen (SVMs) werden von den vShield Endpoint-Partnern bereitgestellt und auf jedem virtuellen vSphere-Desktophost installiert. Die virtuellen Sicherheitsmaschinen führen sicherheitsrelevante Vorgänge für alle virtuellen Desktops aus, die sich auf dem vSphere-Host befinden. Die virtuellen Sicherheitsmaschinen und damit verbundene Komponenten sind erforderliche Komponenten der vShield Endpoint-Plattform.

Überprüfen der vShield Endpoint-Funktion

Nachdem Sie alle erforderlichen Komponenten der vShield Endpoint-Plattform installiert und konfiguriert haben, überprüfen Sie die Funktion der Plattform vor der Bereitstellung der virtuellen Desktops.

Überprüfen Sie mithilfe der vom vShield Endpoint-Partner bereitgestellten Dokumentation die Funktion der vShield Endpoint-Plattform mit dem Master Image des virtuellen Desktops.

Einrichten von VMware Workspace

In diesem Abschnitt finden Sie Informationen zur Einrichtung und Konfiguration von VMware Workspace für die Lösung. Für eine Neuinstallation von Workspace empfiehlt VMware, dass Sie die Aufgaben in der in Tabelle 18 angegebenen Reihenfolge durchführen.

Zusätzlich zu den Referenzen, die in diesem Abschnitt enthalten sind, bietet die VMware Workspace-Dokumentation die zusätzlichen Informationen, die erforderlich sind, um die Installation und Konfiguration der VMware Workspace abzuschließen.

Hinweis: EMC empfiehlt, die VMware Workspace vApp in dem Pool der VSPEX Private Cloud zu installieren.

Tabelle 18. Aufgaben beim Einrichten von VMware Workspace

Aufgabe	Beschreibung	Referenz
Erstellen eines vCenter-IP-Pools	Erstellen Sie den IP-Pool, der von Horizon Workspace zum Zuweisen der IP-Adressen zu den Appliances während der Erstkonfiguration verwendet wird.	Erstellen eines vCenter-IP-Pools
Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen	Weisen Sie die vier IP-Adressen zu, die zum Konfigurieren der virtuellen VMware Workspace-Appliances erforderlich ist. Die IP-Adressen müssen sich von den im IP-Pool verwendeten IP-Adressen unterscheiden.	Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen



Aufgabe	Beschreibung	Referenz
Gewähren der SMTP-Relayberechtigungen für die Workspace data-va-Appliance	Gewähren Sie der Appliance SMTP-Relayberechtigungen, sodass sie SMTP-Meldungen bezüglich Benutzerkonteninformationen und Warnmeldungen senden kann.	• Gewähren der SMTP-Relayberechtigungen für VMware Workspace • E-Mail-Serverdokumentation
Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für VMware Workspace	Konfigurieren Sie eine Datenbank für die Verwendung durch VMware Workspace zum Speichern kritischer Konfigurationsinformationen. Eine externe Datenbank wird aus Performance- und Skalierungsgründen empfohlen.	Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für
Konfigurieren einer CIFS-Freigabe zur Verwendung als VMware ThinApp-Repository (optional)	Konfigurieren Sie optional eine Dateifreigabe mit schreibgeschützten Berechtigungen für VMware Workspace zum Aktivieren der Verteilung von Anwendungen in einem Paket mit ThinApp.	• Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional) • *EMC VNX5400 Unified – Installationshandbuch* • *Installationshandbuch für EMC VNX5600 Unified* • *Leitfaden für die ersten Schritte mit dem EMC Unisphere-System*
Verifizieren der angegebenen E-Mail-Adressen aller Workspace-Benutzer	Verifizieren Sie, dass alle Workspace-Benutzer E-Mail-Adressen angegeben haben.	Überprüfen der angegebenen E-Mail-Adressen aller VMware Workspace-Benutzer
Bereitstellen der VMware Workspace vApp in vCenter	Stellen Sie die VMware Workspace vApp bereit, die als OVA-Datei geliefert wird und die Dateien enthält, die erforderlich sind, um die VMware Workspace-Appliances bereitzustellen.	Bereitstellen der VMware Workspace vApp in vCenter
Anpassen der technischen Daten der virtuellen VMware Workspace-Maschine (für Umgebungen, die mehr als 1.000 Clients hosten)	Stellen Sie die virtuellen VMware Workspace-Maschinen service-va, data-va und gateway-va mit zusätzlichen RAM- und CPU-Ressourcen für Umgebungen von mehr als 1.000 Benutzern bereit.	Anpassen der virtuellen VMware Workspace-Maschinenspezi-fikationen

Aufgabe	Beschreibung	Referenz
Erstellen eines Active Directory-Kontos, das für die VMware Workspace Active Directory-Integration verwendet wird	Erstellen Sie ein Active Directory-Konto, damit VMware Workspace Kontodaten synchronisieren kann. Das Konto muss sich in der Active Directory- Organisationseinheit (OE) befinden, die die VMware Workspace-Zielbenutzer umfasst.	Anbieterdokumentation
Erlangen der Informationen, die erforderlich sind, um die VMware Workspace-Integration mit Active Directory zu aktivieren	Holen Sie sich die Active Directory-Konfigurationsinformationen, die dazu erforderlich sind, VMware Workspace den Zugriff auf Active Directory zu ermöglichen.	Erlangen der Informationen, die erforderlich sind, um die VMware Workspace-Integration mit Active Directory zu aktivieren
Erstellen eines Active Directory-Kontos für die VMware Workspace-Integration in vCenter Server	Erstellen Sie ein Active Directory-Konto, das für die VMware Workspace-Integration in vCenter Server verwendet werden soll.	Anbieterdokumentation
Holen Sie sich die Informationen, die erforderlich sind, um die VMware Workspace-Integration mit vCenter zu aktivieren.	Holen Sie sich die folgenden Informationen, die erforderlich sind, um die VMware Workspace-Integration mit vCenter zu aktivieren. • vCenter-Hostname-FQDN • vCenter-Port-Nummer • Benutzername für das zuvor erstellte VMware Workspace vCenter-Integrationskonto • Passwort für das zuvor erstellte VMware Workspace vCenter-Integrationskonto	VMware Workspace-Dokumentation
Erlangen des VMware Workspace-Lizenzschlüssels	Holen Sie sich von VMware den VMware Workspace-Lizenzschlüssel, der die VMware Workspace-Plattform aktiviert.	
Zugreifen auf die VMware Workspace configurator-va-Appliance-Konsole in vCenter	Schließen Sie den Installationsassistenten auf der configurator-va-Appliance ab.	
Verwenden des VMware Workspace-Konfigurator-Webportals zum Abschließen der webbasierten UI-Installation.	Greifen Sie auf das VMware Workspace-Konfigurator-Webportal über *https://configurator-va-FQDN* zu.	



Aufgabe	Beschreibung	Referenz
Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die virtuelle VMware Workspace-Maschine (optional)	Ersetzen Sie das selbst signierte SSL-Zertifikat, das VMware Workspace standardmäßig installiert hat. Das Zertifikat ist nicht vertrauenswürdig für Webclients oder Maschinen, die den Workspace-Softwareclient ausführen.	Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die virtuelle VMware Workspace-Maschine (optional)
Aktivieren der RSA SecurID-Authentifizierung (optional)	Aktivieren Sie optional die RSA SecurID-Authentifizierung über das VMware Workspace-Konfigurator-Webportal unter *https://configurator-va-FQDN*.	RSA-Dokumentation
Konfigurieren des externen Zugriffs auf die VMware Workspace gateway-va-Appliance (optional)	Aktivieren Sie optional externen Zugriff auf die VMware Workspace gateway-va-Appliance.	• Konfigurieren des externen Zugriffs auf das VMware Workspace-Gateway (optional) • Firewall-Herstellerdokumentation
Aktivieren von Horizon View-Integration (optional)	Aktivieren Sie optional die Horizon View-Integration, um Benutzern den Zugriff auf ihre Horizon View-Desktops direkt über das VMware Workspace-Portal zu ermöglichen.	Aktivieren der Horizon View-Integration (optional)
Aktivieren von ThinApp-Paketen (optional)	Aktivieren Sie optional ThinApp-Pakete, damit mithilfe von ThinApp verpackte Anwendungen automatisch an Clients verteilt werden können, die VMware Workspace Agent ausführen, oder nach Bedarf auf Webclients gestreamt werden können.	• *ThinApp – Benutzerhandbuch* • *ThinApp Package.ini-Parameter – Referenzleitfaden*
Aktivieren von Citrix-veröffentlichten Anwendungen (optional)	Aktivieren Sie optional von Citrix veröffentlichte Anwendungen, um die VMware Workspace-Integration in Citrix XenApp zu ermöglichen und Zugriff auf Anwendungen zu bieten, die von dieser Plattform gehostet werden.	Citrix XenApp-Dokumentation
Benutzern erlauben, VMware Workspace-Funktionen zu verwenden	Verwenden Sie das VMware Workspace-Dashboard, um Richtlinien zu erstellen und Active Directory-Benutzern und -Gruppen Zugriff auf VMware Workspace-Funktionen zu gewähren. VMware Workspace-Benutzer verfügen standardmäßig nicht über die Berechtigung, die Funktionen von VMware Workspace zu verwenden.	VMware Workspace-Dokumentaktion

Aufgabe	Beschreibung	Referenz
Erfassen von Anwendungen mithilfe von ThinApp (optional)	Erfassen Sie optional Anwendungen mithilfe von ThinApp und laden Sie sie in das VMware Workspace-ThinApp-Repository hoch, um sie mithilfe von VMware Workspace-Policies für Clients verfügbar zu machen.	• *ThinApp – Benutzerhandbuch* • *ThinApp Package.ini-Parameter – Referenzleitfaden*

Erstellen eines vCenter-IP-Pools

Sie müssen einen vCenter IP-Pool mit vier verfügbaren Adressen konfigurieren, um die Erstkonfiguration der VMware Workspace vApp abzuschließen. Dieser Pool sollte IP-Adressen im TCP-IP-Zielsubnetz für VMware Workspace verwenden und mit den richtigen DNS-Domain- und DNS-Serverwerten konfiguriert werden.

Zuweisen von IP-Adressen und Erstellen von DNS-Datensätzen

Während der Bereitstellung konfiguriert VMware Workspace die Appliances mit den IP-Adressen, die mittels DNS-Suche ermittelt werden. Erstellen Sie die DNS-Datensätze für jede der vier VMware Workspace vApps, bevor Sie die vApps bereitstellen, mithilfe der entsprechenden IP-Adresse für jede. Erstellen Sie sowohl die Forward (A)- als auch die Reverse (PTR)-Datensätze.

Gewähren der SMTP-Relayberechtigungen für VMware Workspace

Die VMware Workspace data-va-Appliance muss dazu in der Lage sein, Nachrichten mit einem SMTP-Server zu übermitteln. Konfigurieren Sie zu diesem Zweck eine vorhandene E-Mail-Adresse und vergewissern Sie sich, dass die data-va-Appliance die erforderlichen Berechtigungen hat.

Konfigurieren einer PostgreSQL- oder Oracle-Datenbank für VMware Workspace

Während der Erstkonfiguration von VMware Workspace werden Sie dazu aufgefordert, die standardmäßige eingebettete PostgreSQL-Datenbank oder eine Datenbank zu verwenden, die auf einem dedizierten Server gehostet wird, auf dem entweder eine unterstützte Version von Oracle oder PostgreSQL ausgeführt wird. EMC empfiehlt, dass Sie einen dedizierten Server verwenden, um die VMware Workspace-Datenbank für Performance- und Managementzwecke zu hosten. Sie müssen die Datenbank vor der Konfiguration von VMware Workspace erstellen, indem Sie die Anweisungen im *VMware Horizon View – Installationshandbuch* auf der VMware-Website befolgen.

Konfigurieren einer CIFS-Freigabe zur Verwendung als ThinApp-Repository (optional)

Wenn Sie VMware Workspace dafür verwenden, Anwendungen bereitzustellen, die mit VMware ThinApp zusammengestellt wurden, erstellen Sie eine CIFS- oder Windows-Share für die Speicherung von Anwendungen. Der Platzbedarf hängt von der Anzahl der Pakete ab, die von der Share gehostet werden.

Wenn Sie VNX dafür verwenden, die Share zu hosten, erstellen Sie das erforderliche Dateisystem innerhalb des Infrastrukturserver-Speicherpools und erstellen Sie dann eine CIFS-Share. VMware Workspace-Benutzer benötigen schreibgeschützten Zugriff auf diese Freigabe, während ThinApp-Administratoren Lese-/Schreibzugriff benötigen, um ThinApp-Pakete zu verwalten.



Überprüfen der angegebenen E-Mail-Adressen aller VMware Workspace-Benutzer

VMware Workspace erfordert, dass alle Benutzer eine E-Mail-Adresse in ihrem Active Directory-Konto angeben. Wenn das Active Directory-E-Mail-Adressfeld leer ist, werden Benutzer nicht für VMware Workspace aktiviert.

Das Active Directory-Konto muss nicht E-Mail-fähig sein. Das ist ein Begriff, der für Unternehmen verwendet wird, die Microsoft Exchange verwenden. Nur VMware Workspace erfordert, dass das Active Directory-E-Mail-Adressfeld des Benutzers eine gültige E-Mail-Adresse enthält.

Bereitstellen der VMware Workspace vApp in vCenter

Wenn Sie die Deploy OVF Template-Funktion in der vCenter-Konsole verwenden, stellen Sie die VMware Workspace vApp bereit. Legen Sie dazu folgende Feldwerte fest:

- **Host/Cluster**: VSPEX Private Cloud-vSphere-Cluster
- **Resource Pool**: VSPEX Private Cloud-vSphere-Cluster
- **Storage**: VSPEX Private Cloud-Datastore
- **Disk Format**: Thin Provisioning
- **Network Mapping**: Zielnetzwerk für die virtuellen Workspace-Maschinen
- **IP Address Allocation**: Behoben

Wenn die VMware Workspace-Umgebung mehr als 1.000 Anwender unterstützt, müssen Sie die Spezifikationen für die virtuellen service-va-, data-va- und gateway-va-Maschinen anpassen, bevor Sie die vApp starten. Informationen zum Vornehmen dieser Änderungen finden Sie unter Anpassen der virtuellen VMware Workspace-Maschinenspezi-fikationen.

Anpassen der virtuellen VMware Workspace-Maschinenspezi-fikationen

In Tabelle 19 enthält Details zu den Mindestanforderungen an die Hardwareressourcen für VMware Workspace-Umgebungen, die mehr als 1.000 Benutzer unterstützen. Diese Empfehlungen gelten auch für alle weiteren virtuellen data-va-Maschinen, die bereitgestellt werden.

Tabelle 19. VMware Workspace für mehr als 1.000 Benutzer: Mindestanforderungen an die Hardwareressourcen

vApp	vCPUs	Arbeitsspeicher (GB)	Festplattenspeicher (GB)
Configurator-va	1	1	5
Service-va	6	8	36
Connector-va	2	4	12
Data-va	6	32	175
Gateway-va	6	32	9

Erlangen der Informationen, die erforderlich sind, um die VMware Workspace-Integration mit Active Directory zu aktivieren

VMware Workspace erfordert, dass sich die Active Directory-Benutzerkonten in einer anderen Organisationseinheit als der OE der Standardbenutzer befinden. Beschaffen Sie sich die folgenden Informationen zu dieser Integration:

- Name des Active Directory-Domain Controllers und FQDN
- Active Directory-Kontext für die Anbindung, also das Stammverzeichnis der Active Directory-Organisationseinheit, die VMware Workspace-Benutzer und -Gruppen enthält, z. B.:

  OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Active Directory-Basis-DN des zuvor erstellten VMware Workspace Active Directory-Integrationskontos, z. B.:

  CN=svc-horizon,OU=HorizonWorkspace,DC=rtp,DC=lab,DC=emc,DC=com
- Passwort für das zuvor erstellte VMware Workspace Active Directory-Integrationskonto
- Active Directory-Benutzername und -Passwort eines Kontos mit Rechten, Computer mit der Domain zu verknüpfen

Verwenden eines vertrauenswürdigen SSL-Zertifikats und eines privaten Schlüssels für die virtuelle VMware Workspace-Maschine (optional)

Sie können ein vertrauenswürdiges SSL-Zertifikat und einen dazugehörigen privaten Schlüssel verwenden, um das VMware Workspace vApp-Standard-SSL-Zertifikat zu ersetzen. Wenn das Zertifikat nicht ersetzt wird, können Clients auf SSL-Validierungsfehler stoßen, wenn sie auf die VMware Workspace-Umgebung zugreifen. Sie benötigen außerdem die Stamm- und Zwischenzertifikate, um den Zertifikataustauschprozess abzuschließen.

Sie können ein einzelnes Platzhalterzertifikat verwenden oder individuelle Personenzertifikate auf jeder virtuellen VMware Workspace-Maschine ersetzen. Die Zertifikate sollten das PEM-Format aufweisen.

Konfigurieren des externen Zugriffs auf das VMware Workspace-Gateway (optional)

VMware Workspace muss über das Internet erreichbar sein, um VMware Workspace als virtuelle gateway-va-Maschine für den externen Zugriff auf Horizon View zu ermöglichen.

Wenn diese Funktion erforderlich ist, konfigurieren Sie den externen Zugriff, wie in *Installieren und Konfigurieren von VMware Workspace Portal* auf der VMware-Website beschrieben.

Aktivieren der Horizon View-Integration (optional)

Wenn VMware Workspace als Gateway für den externen Zugriff auf Horizon View verwendet wird, müssen Sie die Horizon View-Integration aktivieren, indem sie das Konfigurator-Webportal unter *https://configurator-va-FQDN* verwenden.

Einrichten von VMware vRealize Operations Manager for Horizon View

In diesem Abschnitt werden Informationen zum Einrichten und Konfigurieren von VMware vRealize Operations Manager für Horizon View bereitgestellt.
In Tabelle 20 beschreibt die erforderlichen Aufgaben.

Hinweis: EMC empfiehlt, das Betriebssystem-Volume für vRealize Operations Manager für Horizon View-Server in den Pool der VSPEX Private Cloud zu integrieren. Weitere Informationen zur empfohlenen CPU- und Arbeitsspeicherkonfiguration finden Sie in der vRealize Operations Manager-Dokumentation.



Tabelle 20. Für die Installation und Konfiguration von vRealize Operations Manager erforderliche Aufgaben

Aufgabe	Beschreibung	Referenz
Erstellen eines vSphere-IP-Pools für vRealize Operations Manager	Erstellen Sie einen IP-Pool mit 2 verfügbaren IP-Adressen für die vRealize Operations Manager-Analysen und virtuellen Maschinen der Benutzeroberfläche.	• *VMware vRealize Operations Manager for Horizon View – Installations- und Konfigurationshandbuch* • *VMware vRealize Operations Manager for Horizon View – Administratorhandbuch* • *VMware vRealize Operations Manager for Horizon View – Sicherheitshandbuch*
Bereitstellen von vRealize Operations Manager vSphere Application Services (vApp)	Führen Sie die Bereitstellung und Konfiguration der vRealize Operations Manager vApp durch. Passen Sie die Spezifikationen der 2 virtuellen Server, aus denen sich die vRealize Operations Manager vApp zusammensetzt, abhängig von der Anzahl der überwachten virtuellen Maschinen an.	
Angeben des zu überwachenden vCenter-Servers	Geben Sie auf der Hauptweboberfläche von vRealize Operations Manager den Namen des vCenter-Servers an, der die virtuellen Desktops managt.	
Zuweisen der vRealize Operations Manager-Lizenz	Wenden Sie die vRealize Operations Manager for Horizon View-Lizenzschlüssel über das vCenter-Lizenzdienstprogramm an.	
Konfigurieren der SNMP- und SMTP-Einstellungen (optional)	Konfigurieren Sie optional über die Hauptweboberfläche von vRealize Operations Manager alle für Überwachungszwecke erforderlichen SNMP- oder SMTP-Einstellungen.	
Aktualisieren der Einstellungen für den virtuellen Desktop	Aktualisieren Sie die Firewall-Policies und -Services für den virtuellen Desktop, um das vRealize Operations Manager for Horizon View-desktopspezifische Sammeln von Kennzahlen zu unterstützen.	
Erstellen der virtuellen Maschine für den vRealize Operations Manager for Horizon View Adapter-Server	Erstellen Sie eine virtuelle Maschine im vSphere-Client, die als vRealize Operations Manager for Horizon View Adapter-Server verwendet werden soll.	
Installieren des Gastbetriebssystems für den vRealize Operations Manager for Horizon View Adapter-Server	Installieren Sie Windows Server 2012 R2 als Gastbetriebssystem für den vRealize Operations Manager for Horizon View Adapter-Server.	

Aufgabe	Beschreibung	Referenz
Installieren der VMware vRealize Operations Manager for Horizon View Adapter-Software	Führen Sie die Bereitstellung und Konfiguration der vRealize Operations Manager for Horizon View Adapter-Software durch.	
Importieren der vRealize Operations Manager for Horizon View-PAK-Datei	Importieren Sie die vRealize Operations Manager for Horizon View Adapter-PAK-Datei über die Hauptweboberfläche von vRealize Operations Manager.	
Überprüfen der VMware vRealize Operations Manager for Horizon View-Funktionen	Überprüfen Sie die Funktionen von vRealize Operations Manager for Horizon View mit dem virtuellen Desktopmaster-Image.	



Kapitel 5 Lösungsverifizierung

In diesem Kapitel werden die folgenden Themen behandelt:



Übersicht

Nachdem Sie die Lösung konfiguriert haben, führen Sie die in Tabelle 21 aufgeführten Aufgaben durch. So können Sie die Konfiguration und die Funktionen bestimmter Aspekte der Lösung überprüfen und dafür sorgen, dass die Konfiguration die zentralen Verfügbarkeitsanforderungen erfüllt.

Tabelle 21. Aufgaben für das Testen der Installation

Aufgabe	Beschreibung	Referenz
Überprüfen der Installation	Überprüfen Sie, ob geeignete virtuelle Ports auf jedem virtuellen vSphere-Host-Switch vorhanden sind.	*VMware vSphere-Netzwerk – Handbuch*
	Überprüfen Sie, ob jeder vSphere-Host auf die erforderlichen Datastores und VLANs zugreifen kann.	• *Handbuch für VMware vSphere-Speicher* • *VMware vSphere-Netzwerk – Handbuch*
	Überprüfen Sie, ob die vMotion-Schnittstellen auf allen vSphere-Hosts korrekt installiert sind.	*VMware vSphere-Netzwerk – Handbuch*
Bereitstellen und Testen einer einzigen virtuellen Maschine	Stellen Sie eine einzige virtuelle Maschine über die vSphere-Oberfläche bereit und nutzen Sie dabei die Anpassungsspezifikation.	• *VMware vCenter Server- und Hostverwaltung – Handbuch* • *VMware vSphere für virtuelle Maschinen – Managementhandbuch*
Überprüfen der Redundanz der Lösungskomponenten	Starten Sie nacheinander jeden Speicherprozessor neu und vergewissern Sie sich, dass die VMware-Datastores-Verbindung aufrechterhalten wird.	Überprüfen der Redundanz der Lösungskomponenten
	Deaktivieren Sie nacheinander jeden der redundanten Switche und überprüfen Sie, ob die Verbindung von vSphere-Host, virtueller Maschine und Speicherarray erhalten bleibt.	Anbieterdokumentation
	Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine erfolgreich zu einem alternativen Host migrieren kann.	*VMware vCenter Server- und Hostverwaltung – Handbuch*
Provisioning der verbleibenden virtuellen Desktops	Stellen Sie Desktops über die verknüpften View Composer-Clones oder die vollständigen virtuellen Maschinen bereit.	*VMware Horizon View – Administratorhandbuch*



Checkliste nach der Installation

Die folgenden Konfigurationsaufgaben sind für die Funktion der Lösung von zentraler Bedeutung. Vergewissern Sie sich, dass die Aufgaben abgeschlossen sind, bevor Sie diese Lösung für die Produktion bereitstellen. Überprüfen Sie Folgendes auf jedem vSphere-Server, der als Teil dieser Lösung verwendet wird:

- Die vSwitches, die die Client-VLANs hosten, sind mit ausreichend Ports konfiguriert, um die maximale Anzahl virtueller Maschinen zu beherbergen, die ein Host beherbergen kann.
- Alle erforderlichen virtuellen Maschinenportgruppen sind konfiguriert, und jeder Server kann auf die erforderlichen VMware-Datastores zugreifen.
- Eine Schnittstelle ist korrekt für vMotion konfiguriert. Weitere Informationen finden Sie im *VMware vSphere-Netzwerkleitfaden*.

Weitere Informationen finden Sie in den in Referenzdokumentation aufgeführten Dokumenten.

Bereitstellen und Testen einer einzigen virtuellen Maschine

Stellen Sie eine virtuelle Maschine bereit, um den Betrieb der Lösung zu überprüfen. Überprüfen Sie, ob die virtuelle Maschine der entsprechenden Domain zugeordnet ist, Zugriff auf die erwarteten Netzwerke hat und es möglich ist, dass Sie sich bei ihr anmelden.

Überprüfen der Redundanz der Lösungskomponenten

Testen Sie bestimmte Szenarien, die für die Wartung oder Hardwareausfälle relevant sind, wie in diesem Abschnitt beschrieben, um zu überprüfen, ob die verschiedenen Komponenten der Lösung die Verfügbarkeitsanforderungen erfüllen.

XtremIO

Starten Sie nacheinander jeden XtremIO-Speicher-Controller neu und vergewissern Sie sich, dass die VMFS-Datastores-Verbindungen aufrechterhalten werden.

1. Melden Sie sich mithilfe des **xinstall**-Kontos beim Speicher-Controller A an.
2. Starten Sie den Controller mit der Option **6** unter **Install** in der Menüleiste neu.
3. Überprüfen Sie während des Neustartzyklus das Vorhandensein von VMFS-Datastores auf vSphere-Hosts.
4. Mithilfe der XtremIO-Speichermanagement-Anwendungsoberfläche überprüfen Sie, ob Speicher-Controller A online geschaltet wird, indem er das **Warnmeldungsfenster** oder die **Hardware** überwacht.
5. Wiederholen Sie dieses Verfahren für Speicher-Controller B.

Isilon

Wenn Isilon als Teil der Lösung bereitgestellt wird, starten Sie nacheinander jeden Isilon-Node neu und vergewissern Sie sich, dass die Verbindungen mit den CIFS-Dateisystemen erhalten bleiben:

1. Stellen Sie eine Verbindung zu einem verfügbaren Node in dem Cluster mit einem seriellen Kabel oder einem Netzwerkkabel her.
2. Führen Sie den Befehl **isi status –q** aus, um die IP-Adresse des Node zu bestimmen, den Sie herunterfahren.
3. Führen Sie auf dem Node, mit dem Sie verbunden sind, den Befehl **ssh** aus, um eine SSH-Verbindung mit dem Node herzustellen, der heruntergefahren werden soll.
4. Führen Sie den Befehl **shutdown -p now** aus, um den Node herunterzufahren.
5. Führen Sie den Befehl **isi status -q** aus, um zu prüfen, ob der Node heruntergefahren ist.

   Der Node sollte den Status **D--R** (Down, Read Only) haben. Sehen Sie sich die Node-ID **3** im folgenden Beispiel an:

   ID |IP Address |DASR| In Out Total| Used / Size | Used / Size

   ---+---------------+----+-----+-----+-----+------------------+-

   1|10.53.217.201 | OK | 48M| 0| 48M| 19G/ 6.2T(‹ 1%)|(No SSDs)

   2|10.53.217.202 | OK | 46M| 0| 46M| 23G/ 6.2T(‹ 1%)|(No SSDs)

   3|10.53.217.203 |D--R| n/a| n/a| n/a| n/a/ n/a(n/a)| n/a/n/a(n/a)

6. Während der Node heruntergefahren ist, vergewissern Sie sich, dass der Zugriff auf die CIFS-Dateisysteme wiederhergestellt wird oder erhalten bleibt.
7. Schalten Sie den Node ein, der in Schritt 4 heruntergefahren wurde, und führen Sie dann Schritt 5 erneut aus und vergewissern Sie sich, dass der Node nun wieder den Status **OK** hat.
8. Wiederholen Sie die Schritte 2 – 7 für die anderen Isilon-Nodes im Cluster.

VNX

Wenn VNX als Teil der Lösung bereitgestellt wird, führen Sie die folgenden Überprüfungsaufgaben durch.

1. Starten Sie jeden VNX-Speicherprozessor nacheinander neu und überprüfen Sie, ob die Verbindungen zu den CIFS-Dateisystemen aufrechterhalten werden:
   a. Melden Sie sich mit Administratorrechten bei der Control Station an.
   b. Wechseln Sie zu **/nas/sbin**.
   c. Geben Sie den folgenden Befehl ein, um SP A neu zu starten.
      ```
      ./navicli -h spa rebootsp
      ```
   d. Überprüfen Sie während des Neustartzyklus die Präsenz von Datastores auf vSphere-Hosts.
   e. Wenn der Zyklus abgeschlossen ist, geben Sie den folgenden Befehl ein, um SP B neu zu starten:
      ```
      ./navicli -h spb rebootsp
      ```




2. Führen Sie nacheinander ein Failover für jeden VNX-Data Mover durch und überprüfen Sie, ob die Verbindungen zu den CIFS-Dateisystemen wiederhergestellt werden.

   a. Geben Sie an der Eingabeaufforderung **$** der Control Station den folgenden Befehl ein, wobei Sie *movername* durch den Namen des Data Mover ersetzen:

      ```
      server_cpu movername -reboot
      ```

   b. Überprüfen Sie, ob die Netzwerkredundanzfunktionen erwartungsgemäß funktionieren, indem Sie nacheinander die redundanten Switching-Infrastrukturen deaktivieren. Während jede der Switching-Infrastrukturen deaktiviert ist, überprüfen Sie, ob alle Komponenten der Lösung die Verbindung miteinander und zu jeder vorhandenen Clientinfrastruktur aufrechterhalten.

   c. Starten Sie über die Unisphere-Benutzeroberfläche das System neu.

vSphere-Host

Aktivieren Sie auf einem vSphere-Host, der mindestens eine virtuelle Maschine enthält, den Wartungsmodus und überprüfen Sie, ob die virtuelle Maschine zu einem alternativen Host migrieren kann.



Kapitel 6 Referenzdokumentation

In diesem Kapitel werden die folgenden Themen behandelt:



EMC Dokumentation

Die folgenden Dokumente auf http://germany.emc.com oder der EMC Online Support-Website bieten zusätzliche und relevante Informationen. Der Zugriff auf diese Dokumente hängt von Ihren Anmeldedaten ab. Falls Sie auf ein Dokument nicht zugreifen können, wenden Sie sich an Ihren EMC Vertriebsmitarbeiter.

- *EMC XtremIO-Speicherarray – Benutzerhandbuch*
- *EMC XtremIO-Speicherarray – Bedienungsanleitung*
- *EMC XtremIO-Speicherarray: Softwareinstallation und Upgrade – Handbuch*
- *EMC XtremIO-Speicherarray: Hardwareinstallation und Upgrade – Handbuch*
- *EMC XtremIO-Speicherarray – Sicherheitskonfigurationsleitfaden*
- *EMC XtremIO-Speicherarray – Checkliste für Aufgaben vor der Installation*
- *EMC XtremIO-Speicherarray – Handbuch zur Vorbereitung des Aufstellorts*
- *Installationshandbuch für EMC VNX5400 Unified*
- *Installationshandbuch für EMC VNX5600 Unified*
- *EMC VNX Installation Assistant for File/Unified-Arbeitsblatt*
- *EMC VNX FAST Cache: ein detaillierter Überblick, White Paper*
- *EMC VNX Unified: Best Practices für Performance – Leitfaden zur Anwendung von Best Practices*
- *EMC VSI für VMware vSphere Web Client – Produktleitfaden*
- *X400-Installationshandbuch*
- Managen von KMU-Shares und Benutzer-Home-Verzeichnissen in EMC Isilon OneFS 6.5 und höher
- *Bereitstellung von virtuellen Microsoft Windows 8-Desktops – Leitfaden zur Anwendung von Best Practices*
- *Installations- und Administrationshandbuch für PowerPath/VE für VMware vSphere*
- *EMC PowerPath Viewer – Installations- und Administrationshandbuch*
- *Design- und Implementierungsleitfaden – EMC Backup und Recovery für VSPEX-Anwender-Computing für VMware Horizon View*
- *Sicherung des EMC VSPEX-Anwender-Computings mit RSA SecurID: VMware Horizon View 5.2 mit VMware vSphere 5.1 für bis zu 2.000 virtuelle Desktops – Designleitfaden*

Andere Dokumentationen

Die folgende Dokumentation auf der VMware-Website enthält weitere und relevante Informationen:

- *Installations- und Einrichtungshandbuch für VMware vSphere*
- *VMware vSphere-Netzwerk – Handbuch*
- *VMware vSphere-Ressourcenverwaltung – Handbuch*



- *Handbuch für VMware vSphere-Speicher*
- *VMware vSphere für virtuelle Maschinen – Administratorhandbuch*
- *VMware vCenter Server- und Hostverwaltung – Handbuch*
- *Installieren und Verwalten von VMware vSphere Update Manager*
- *Vorbereiten der Update Manager-Datenbank*
- *Vorbereiten der vCenter Server-Datenbanken*
- *Management von Arbeitsspeicherressourcen in VMware vSphere 5*
- *VMware Horizon View – Administratorhandbuch*
- *VMware Horizon View – Planungshandbuch*
- *VMware Horizon View – Installationshandbuch*
- *VMware Horizon View – Integrationshandbuch*
- *VMware Horizon View – Profilmigrationshandbuch*
- *VMware Horizon View – Sicherheitshandbuch*
- *VMware Horizon View – Upgrade-Handbuch*
- *VMware Horizon View 6.0 – Versionshinweise*
- *VMware Horizon View – Optimierungshandbuch für Windows 7 und 8 (White Paper)*
- *Installieren und Konfigurieren von VMware Workspace Portal*
- *Upgrade von VMware Workspace*
- *VMware Workspace – Administratorhandbuch*
- *VMware Workspace Portal – Benutzerhandbuch*
- *VMware vRealize Operations Manager für Horizon View – Installations- und Konfigurationshandbuch für Windows und Linux*
- *VMware vRealize Operations Manager for Horizon View – Administratorhandbuch*
- *VMware vRealize Operations Manager for Horizon View – Sicherheitshandbuch*
- *VMware vShield – Administratorhandbuch*
- *VMware vShield – Kurzanleitung*

Die folgende Dokumentation auf der Microsoft TechNet-Website enthält weitere relevante Informationen:

- *Installieren und Bereitstellen von Windows Server 2012 R2*
- *SQL Server-Installation (SQL Server 2012)*



Anhang A Konfigurationsarbeitsblatt

In diesem Anhang wird das folgende Thema behandelt:

Arbeitsblatt für die Kundenkonfiguration

Bevor Sie die Lösung konfigurieren, müssen Sie einige kundenspezifische Konfigurationsinformationen wie IP-Adressen, Hostnamen usw. erfassen.

In den folgenden Tabellen (Tabelle 22 bis einschließlich Tabelle 29) ist ein komplett leeres Arbeitsblatt enthalten, das Sie zur Aufzeichnung dieser Informationen verwenden können.

Um die Kundenangaben zu bestätigen, können Sie dieses Arbeitsblatt mit dem folgenden EMC VNX-Konfigurationsarbeitsblatt abgleichen: *EMC VNX Installation Assistant for File/Unified-Arbeitsblatt*.

Tabelle 22. Allgemeine Serverinformationen

Servername	Zweck	Primäre IP-Adresse
	Domain-Controller	
	Primäres DNS	
	Sekundäres DNS	
	DHCP	
	NTP	
	SMTP	
	SNMP	
	VMware vCenter-Konsole	
	VMware Horizon View Connection Server	
	Microsoft SQL Server	
	VMware vShield Manager	
	Managementserver für die Virenschutzlösung	
	vRealize Operations Manager for Horizon View Adapter-Server	

Tabelle 23. vSphere-Serverinformationen

Server name	Zweck	Primäre IP-Adresse	Private Netzadressen (Speicher)	VMkernel-IP-Adresse	vMotion-IP-Adresse
	vSphere-Host 1				
	vSphere-Host 2				
	...				



Tabelle 24. XtremIO-Arrayinformationen

Feld	Wert
Arrayname	
XMS-IP	
IP-Adressen des Speicher-Controllers	
Initiatorgruppennamen	
Datastore-Namen	

Tabelle 25. VNX-Arrayinformationen

Feld	Wert
Arrayname	
Administratorkonto	
Management-IP-Adresse	
Name des Speicherpools	
CIFS-Share-Name	

Tabelle 26. Isilon-Arrayinformationen

Feld	Wert
Arrayname	
Administratorkonto	
Management-IP-Adresse	
Subnetzname	
Subnetz-IP-Pool	
SmartConnect-Zonenname	
Zugriffszonenname	
CIFS-Share-Name	

Tabelle 27. Informationen zur Netzwerkinfrastruktur

Name	Zweck	IP address	Subnetzmaske	Standard-Gateway
	Ethernetswitch 1			
	Ethernetswitch 2			
	...			

Tabelle 28. VLAN-Informationen

Name	Zweck des Netzwerks	VLAN-ID	Zugelassene Subnetze
	Clientzugriffsnetzwerk		
	Speichernetzwerk		
	Managementnetzwerk		

Tabelle 29. Servicekonten

Konto	Zweck	Passwort (optional, angemessen gesichert)
	Windows Server-Administrator	
Root	VMware vSphere-Root	
Root	XtremIO-Array-Root-Konto	
xmsupload	XtremIO-Array-xmsupload-Konto	
Technische	XtremIO-Array-XMCLI-Tech-Konto	
Root	VNX-Array-Root	
	Arrayadministrator	
	VMware vCenter-Administrator	
	VMware Horizon View-Administrator	
	Microsoft SQL Server-Administrator	
	VMware vRealize Operations Manager-Administrator	
	VMware vShield Manager-Administrator	